Humans and Vulnerability During Times of Change: Computer Security Needs, Practices, Challenges, and Opportunities

Lucy Simko

A dissertation
submitted in partial fulfillment of the
requirements for the degree of

Doctor of Philosophy

University of Washington

2022

Reading Committee:

Tadayoshi Kohno, Chair

Yasemin Acar

David Kohlbrenner

Franziska Roesner

Program Authorized to Offer Degree:
Paul G. Allen School of Computer Science & Engineering

University of Washington

Abstract

Humans and Vulnerability During Times of Change:
Computer Security Needs, Practices, Challenges, and Opportunities

Lucy Simko

Chair of the Supervisory Committee:
Professor Tadayoshi Kohno
Paul G. Allen School of Computer Science & Engineering

This dissertation explores the relationship between *change* and vulnerability to security and privacy harms. I suggest that change causes vulnerability in part due to the nature of change, and in part due to the design of technical and sociopolitical systems. I suggest that this connection between change and vulnerability exists for three reasons. First, when someone experiences change, new or different threats, risks, assets, technologies, and actors arise; if they do not update their personal threat model, it may be incomplete or inaccurate, making them unable to respond to emergent threats. Second, even if they are aware of all threats, they may be unable to prioritize security and privacy, as other needs may be more important. Third, the design of technology and user education is often misaligned with the needs and threat models of those going through change, causing vulnerable populations to become more vulnerable and exacerbating existing systemic inequities.

I explore these three themes through four populations experiencing immense change differing in scope, cause, and time frame: (a) refugees who have moved to the United States; (b) activists in Sudan during the 2018-2019 revolution; (c) people considering using contact tracing apps during the first months of the Covid-19 pandemic; and (d) people who experience hurricanes.

This dissertation makes contributions at two levels. First, each individual research chap-

ter contributes an understanding of the security and privacy needs, experiences, and challenges of vulnerable populations. In each chapter, I make design, policy, and research recommendations to work towards more equitable technology. Second, taken together, the entirety of this dissertation contributes a deep understanding of the relationship between *change* and *vulnerability* to computer security and privacy harms. While the nature of change itself *does* engender vulnerability, in many ways the vulnerability is constructed—by sociopolitical and historical injustices or by technical design, or both.

TABLE OF CONTENTS

ACKNOWLEDGMENTS

The past seven years have been a journey. I'm incredibly grateful that my work has been a place of comfort, strength, and escape, and that of all the stress I have faced throughout grad school, the biggest stressor has rarely been doing a PhD. Much of this is thanks to Yoshi Kohno's kindness and determination to support me. Thank you, Yoshi, for your support, but also for your enthusiasm and creativity, and for teaching me to love research in my own way.

I'm also incredibly grateful to Franzi Roesner for being an invaluable resource and mentor throughout my time at UW, and to Yasemin Acar for mentoring me through the last year of my PhD. Thank you both for your support and insight about research and life outside research. Thank you also to Sara Sprenkle for starting me on this journey and for helping me grow as a person and a learner.

I've been lucky to have many other brilliant collaborators over the years, to whom I am very thankful: faculty Alex Bardas, Ryan Calo, and Luke Zettlemoyer, graduate students Ada Lerner, Samia Ibtasam, and Alaa Daffalla, and undergraduate students Jack Lucas Chang, Maggie Jiang, Jonathan Qassis, and Carmen Hanish. I am very fortunate to have worked with you. Thank you for everything I've learned about your fields of study, your ways of looking at the world, and your styles of collaboration and mentorship. You've all made me a better researcher and collaborator.

I'm also incredibly thankful for all of the administrative support at UW, especially Elise deGoede Dorough, Joe Eckert, Dali Grubisa, and Melody Kadenko. Thank you for always answering all of my questions and helping me through grad school.

I also could not have gotten by without a little help from my friends. UWers, thank you for inspiring me to think about research in new ways and to think about things *other* than research. I'm particularly thankful to have had Camille Cobb, Chris Geeng, Kiron Lebeck, Anna Kornfeld Simpson, and Eric Zeng in my corner throughout my entire time at UW: thank you all for making me laugh a lot. Thank you for bringing me joy, inspiration, fun, and food. Specifically: Anna, thank you for your unbelievable ability to become incredibly excited about someone else's research; you've reignited my excitement and helped me past research and writing problems so many times. Cam, thank you for always answering my calls, talking endlessly with me, and for telling me why everything's going to be ok. Kiron, my walking buddy, I miss you. Thank you for always being up for a break from work and for excellent food. Eric, thank you for always having a hot take and for being absolutely hilarious and sincere at the same time. And for sharing your adventures!

Thank you also to all the members of the UW Security and Privacy lab that I've had the pleasure to be friends with and work with over the years, particularly Ada Lerner, Peter Ney, Kimberly Ruth, Kentrell Owens, Kaiming Cheng, Miranda Wei, Tina Yeung, Michael Flanders, Karl Koscher, Shri Mare, Earlence Fernandes, Ivan Evtimov, Paul Vines, and Alex Takakuwa.

I'm also grateful to my friends outside UW for keeping me grounded and reminding me that the world is a giant and awesome place. Thanks to Maria for always being there for me and telling me exactly what I need to hear. Thank you, Kristina and Michael, for all the conversations and adventures (even that one snowshoeing trip, you know the one). Thank you also to Jessica, Zane, and Penelope for being our first friends in Seattle, and for continuing a friendship across timezones. Thank you to Chris, Kiwi, and Charles for always supporting my podcast.

I also would not have gotten here without my family, whom I love so much. Thanks, Mom and Dad, for always listening to me talk about research and only once asking "is this really computer science?" Thank you for your endless support and love. Theo, you are brilliant and you inspire me. Thanks for always holding me (and everyone else) to high standards. Nana and Bubba—thank you for being who you are and, in doing so, being the absolute coolest and most generous people I know.

Finally, someone who fits in all of these categories: thank you, Karl, for being here with me through the best and the worst of it. I could not have done this without you.

DEDICATION

To my family and friends, who inspire me.

Chapter 1
INTRODUCTION

Computer security and privacy is an omnipresent challenge for those who use technology. However, computer security and privacy mechanisms are often confusing, frustrating, or unusable due to designs misaligned with users' needs and mental models [257, 267, 320]. These design misalignments can lead to security and privacy *harms*, for example, gaps in the confidentiality, integrity, or availability of one's communications, adversarial parties gaining access to data, or data loss. While security and privacy harms can be damaging or dangerous for everyone, vulnerable and marginalized populations can face higher risks and more determined adversaries. For example, any lapse in security and privacy of communications could lead to minor embarrassment, but for queer youth in a region where they could be persecuted (or prosecuted) because of their identity, a gap in privacy or security could have serious consequences [107]. This dissertation adds to a growing body of work that studies the security and privacy practices, needs, and experiences of vulnerable or marginalized populations in order to better align security and privacy design with the needs of these populations, which will benefit others as well.

In my dissertation, I identify one specific aspect of vulnerability—change—and focus on the relationship between *change* and vulnerability to computer security and privacy harms. I explore *why* change makes people vulnerable to security and privacy harms, finding that **in some ways, the very nature of change makes one vulnerable, but in many ways, the vulnerability is constructed, by sociopolitical and historical injustices, or by technical design, or both**. I follow this relationship between change and computer security in four populations: refugees who have resettled to the US (Chapter 2), Sudanese activists during the 2018-2019 revolution (Chapter 3), a multi-national population during the early months of the Covid-19 pandemic (Chapter 4), and people in the US who have experienced hurricanes (Chapter 5).

As many have argued, including Ruha Benjamin in *Race After Technology* [33], the concepts of sociopolitical systems, technical systems, and race are indelibly intertwined, and deserve to be treated as such in order to right injustices caused by technical design. However, it is useful to distinguish which elements of vulnerability are caused *directly* by ill-fitted technical design, with the understanding that this design may have as its root cause sociopolitical inequities and systemic racism.

Scope: change. The type of changes I explore in this dissertation are big changes that are or could be life-altering, either temporarily or permanently, by significantly changing one's daily routines, sense of personal safety and security, personal and professional relationships, financial security, and health or physical safety. Though systematically defining and categorizing change is out of scope for this work, I have studied populations experiencing changes that are different in terms of cause, time frame, and scope. **I explore the following three themes about change and vulnerability to security and privacy harms:**

(1) Change creates different elements of one's threat model—actors, threats, assets—as well as different technical needs. By definition, change involves the emergence and disappearance of assets, actors, threats, risks, technologies, and needs. In order to avoid having incomplete threat models, this means that individuals must have complete knowledge about their world at all times throughout the change and update their threat model and actions accordingly immediately. This is, at best, impractical and, at worst, impossible. Incomplete threat models, made more so by change, are a theme throughout the work presented in the following chapters, and can lead users to create inappropriate security and privacy goals or to take actions that do not match with their goals.

(2) During a period of change, people may change how they prioritize computer security and privacy in response to other emergent needs. Even if someone has a complete and accurate threat model, they may not prioritize security and privacy because the threats or rewards posed by something else are stronger or more urgent. Users may also *increase* their prioritization of security and privacy in response to change. Broadly speaking, these choices that users make to prioritize security and privacy at the expense of other needs—or to deprioritize security and privacy—are often forced upon them by misaligned technical designs or incomplete threat models. These trade-offs are often not technically necessary, which leaves opportunities for the technical community to better design tools and user outreach.

(3) When technology design is misaligned with the needs and uses of marginalized populations, it causes those populations to have to work harder to maintain security and privacy, exacerbating existing systemic inequalities during times of change. Prior work has well-documented design misalignments that cause non-WEIRD or marginalized populations to become more vulnerable to security and privacy issues [47, 194, 246, 316]. Each chapter of this dissertation adds to this body of work, and, taken together, point to technology design misalignments that exacerbate existing systemic inequalities.

Furthermore, marginalized populations are more likely to experience or be hit harder by these types of change, instability, or crisis. For example, Black communities in the US experienced higher rates of Covid-19 infection and worse outcomes [155], and communities of people who are racially minoritized or poor receive less aid during natural disasters [91]. Technology design that is misaligned with the needs of populations going through change make already-vulnerable populations more vulnerable.

1.1 Contributions and summary

Through my work with four populations I explore these themes about the nature of change, security and privacy, and design, summarized in Table 1.1.

Chapter 2 is about how refugees in the US use technology to accomplish their goals, and is a version of a paper published at 2018 IEEE Symposium on Security and Privacy with coauthors Ada Lerner, Samia Ibtasam, Franziska Roesner, and Tadayoshi Kohno [271]. Refugees who have resettled to the US have gone through a significant life change (moving countries) and may experience systemically-enforced forms of instability like financial insecurity. Through interviews and focus groups, we find that refugees are incentivized or forced to use new technologies (e.g., email) to apply for jobs and for government benefits; that they receive significant support from their caseworkers but that they do not always trust their caseworkers; and that they acquire a bevy of new types of information to protect once in the US (theme 1). We observe that they cannot always prioritize security and privacy when they want to, e.g., by having their email password under someone else's control (theme 2), and that many of the authentication mechanisms they encounter make cultural and linguistic assumptions that do not fit them, at best costing them time, and at worst leading them to take security and privacy measures that do not match with their threat models (theme 3).

Chapter 3 explores political revolution as change, through interviews with activists about the Sudanese revolution in 2018-2019, in a version of a paper published at IEEE Security and Privacy 2021 with co-lead-author Alaa Daffalla, and co-authors Tadayoshi Kohno and Alex Bardas. Political activists *drive* change, and also experience instability during a revolution, including economic instability and physical insecurity. We found that the activists faced new or increased threats from government adversaries, such as internet blackout, censorship, electronic surveillance, and search of personal electronics after arrest. Though these threats may have existed before the revolution, they were more salient during the revolution (theme 1). At a high level, we observed that participants' use of technology was driven by political and social context, and that there were mismatches between technology design and the political and social context in Sudan during the revolution (theme 3). Some of these design mismatches forced participants to take risks in order to advance the revolution and achieve their political goals, even though they expressed that they wanted to prioritize digital safety and privacy (theme 2).

Chapter 4 explores change through the first months of the Covid-19 pandemic, a global change, in a version of a paper published in ACM's Digital Threats: Research and Practice (DTRAP) Journal in 2021 with co-authors Jack Chang, Maggie Jiang, Ryan Calo, Franziska Roesner, and Tadayoshi Kohno [270]. This chapter is about public opinion towards automated contact tracing during the first months of the global pandemic, a time of great change for almost everyone: increased health risks, many unknowns about the virus itself, changed social norms, different technologies (e.g., contact tracing apps), and, for many, financial insecurity [169]. In the first few months of the pandemic, contact tracing apps and their potential to lessen the spread were a topic of public discussion, and when contact tracing apps were first released, they were new technologies released into a world already experiencing a lot of societal change (theme 1). In a series of surveys over six months with a multi-national population, we found that individuals weighed security and privacy against other risks—e.g., health—when deciding whether to install a contact tracing app (theme 2). Participants also brought up concerns about contact tracing apps as a vector for surveillance on marginalized groups, now or in the future (theme 3).

Chapter 5 explores hurricanes as a regional change, and considers technology *access* as a prerequisite for computer security and privacy. In this project we explore technology use holistically during hurricanes, in forthcoming work with Harshini Sri Ramulu, Tadayoshi Kohno, and Yasemin Acar. Hurricanes regularly affect people around the world and can destroy physical infrastructure, disrupt people's ability to work (causing financial insecurity), obtain resources (causing food insecurity), and cause personal injury and death. Through a series of surveys during the 2021 hurricane season with people who live in coastal areas of the continental US, we found that people's needs change during a hurricane, as do both their ability to complete them and the risks of not completing them, e.g., local communication may become more important for physical safety, but may be harder to complete due to power, internet, and electrical outages (theme 1). We found that participants prioritized some needs and uses of technologies over others, for example, by rationing electricity or cellular data when infrastructure had been damaged or destroyed. Participants rarely mentioned computer security and privacy concerns, but, as security and privacy researchers, we note the criticality of the technology they were able to use, and make recommendations toward increasing security, privacy, preparedness, and resilience at a number of levels (theme 2). We also observe that communities that are already marginalized by systemic sociopolitical inequalities are historically harder hit by natural disasters [91], and that the existing literature about technology use during crises misses an opportunity to help the communities that have less access to technology and reliable infrastructure. We also speculate about design recommendations that would align more closely with resource-constrained users' needs during disasters (theme 3).

Finally, Chapter 6 returns to the broader themes about change and vulnerability as they appeared in each preceding chapter of research, and suggests future directions for researchers, designers, technologists about both *designing for change* and about *aspects of vulnerability other than change.* Individually, Chapters 2-5 contribute an understanding of how certain populations experience and think about security, privacy, safety, and technology use. As a whole, this dissertation contributes a deep understanding of one aspect of vulnerability—change—and explores how technology design that is misaligned with users' needs, particularly users who are already marginalized, contributes to systemic inequity by raising the bar for security and privacy inequitably through ill-fitted design.

1.2 Methodology

Throughout the research in this dissertation, I use primarily qualitative methodologies, with descriptive statistics where appropriate. My coauthors and I chose qualitative methodologies because our research questions were broad, generally about participants' experiences, needs, thoughts, preferences, and technology use [60]. Qualitative methodologies gave participants space to teach us something about themselves that we did not know, or to take the research in another direction. My goal as a qualitative researcher, especially with vulnerable or marginalized populations that I am not a part of, was to treat my participants ethically, to let my participants speak directly to the reader when possible, and to summarize their

	(1) Threat model becomes incomplete due to change, causing vulnerability	**(2) Competing needs change prioritization of security and privacy**	**(3) Design misalignments exacerbate existing systemic inequities**
Refugees in the US: moving countries, financial insecurity	Refugees don't always trust their case managers, encounter unfamiliar scams, acquire new types of information (e.g., SSNs); some use email and computers for the first time.	Financial security: Refugees deprioritize S&P to get a job, housing, etc, or they prioritize S&P using costly workarounds.	Cultural assumptions made by technology make security and privacy harder (e.g., birthdays as authenticators, security questions, password management).
Sudanese activists: political revolution: economic instability, physical security threats, changes in daily routine	A revolution meant a dramatically changing political and technical context: new and increased threats from the adversary (e.g., internet blackout, surveillance).	Political goals: activists had greater need for S&P, but their political goals competed with their need for computer security and physical safety due to issues with usability and group adoption of technology.	Privacy tools or strategies designed for a US context, e.g., forcing passcode authentication, are misaligned due to assumptions about the local definitions of privacy. Also, international sanctions drove technology availability.
People considering contact tracing apps during Covid-19: new health risks, new social mores, new technology	People have misunderstandings about how contact tracing apps work, impacting their ability to make an informed decision about adoption.	Health: when deciding whether to use contact tracing apps, people weigh S&P against potential health benefits for themselves and others.	Participants were concerned about S&P harms to marginalized populations from contact tracing app surveillance and data.
People who experience hurricanes: destruction of property and infrastructure, changes in daily routine	During a hurricane, people use technology when possible, but it is not always possible due to resource constraints. Concerns are broader than digital S&P.	Physical safety: changed needs during the disaster lead to safety, information, and communication needs emerging. Little mention of computer S&P in our data, but we speculate about a number of potential issues.	Little work on technology & disaster focusing on those who are unable to use technology due to infrastructure damage. Hurricanes hit vulnerable communities harder. Technology exacerbates this through design misalignments.
What next? Consider other aspects of vulnerability; design for change.	**Designers:** design for people experiencing change; anticipate new actors, threats, assets, changed circumstances, etc. **Researchers:** continue to amplify the voices of and work with vulnerable and marginalized populations; use the lens of instability, change, and crisis, to identify populations. Continue to deeply engage with the idea of vulnerability and identify *other aspects of vulnerability.* **Non-technical solutions** are critical to addressing sociopolitical systems that reinforce these issues.		

Table 1.1: Summary of work

experiences in an appropriate way that always stays true to what they said.

For two of the populations—refugees and Sudanese activists—we conducted semi-structured interviews and focus groups, qualitative tools commonly used for inquiry into vulnerable or understudied populations, e.g. [47, 197]. For focus group and interview data, we collected data until reaching thematic saturation and followed standard qualitative coding methodologies, creating a hierarchical codebook through iteratively developed open and axial codes. At least two researchers coded every transcript.

For research about contact tracing apps and hurricane survivors, we employed online surveys, in part because they allowed us to quickly recruit a geographically diverse and disparate set of participants, and in part due to pandemic-era research restrictions. Our surveys provide some quantitative data for which we report descriptive statistics, but we consider our data primarily qualitative due its rich, free-form nature. We followed similar qualitative coding practices for the free-form data as for transcripts.

Ethical considerations for research with vulnerable or marginalized populations. Though it is always critical to design human subjects studies ethically, it is especially important when working with populations who are at greater risk for harm, such as vulnerable populations. Participant safety and fairness were paramount throughout each study. Each chapter explores our methodology and ethical considerations further, but we did several things in each study to minimize participant harm:

- **IRB approval.** We obtained approval from the University of Washington's Human Subjects Division (IRB) and additionally from any other institution's IRB that required it. IRB approval is necessary but not sufficient to ensure safe and ethical treatment of participants because of the IRB's narrow definition of vulnerability and harm.

- **Minimize PII and sensitive data collection.** We did not collect unnecessary personally identifying information (PII), and our IRB approved of all the PII that we did collect. For example, in our study of activists, only one researcher had the contact information for each participant, and we did not record any PII as part of the study. We also did not start conversations about sensitive information not related to our research topic, e.g., in our study with refugees, we did not ask about their journeys—which are traumatic for some—unless they brought it up (some did).

- **Let participants decide what to share.** In each study, no questions were mandatory (other than screening questions to ascertain broad eligibility, such as age). For participant safety and comfort, we relied on participants to decide what they felt was safe and appropriate to share, which is especially important with, for example, activists, who knew the threats they faced more than we, the researchers, did. In interviews and focus groups, we reminded participants throughout the study that no questions were mandatory, and we tried to pay attention to non-verbal cues indicating a participant was uncomfortable. In surveys, we made all questions optional and reminded participants in the consent text that they were not obligated to answer every question; we also gave participants a study-specific email address at which they could reach us and answered private messages on the survey recruitment platform.

- **Informed and usable consent.** In each study, we also worked to create a consent process that was understandable to participants and that led to them giving their *informed* consent. In interviews and focus groups, we let participants ask questions about the consent form, us, the research, our expectations for their participation, and their data until they were satisfied with the study (or, until they decided they did not want to participate, which did not happen). In surveys, we wrote intentionally short consent text, in hopes that participants actually read it, and answered questions about the research and their data both through private message on the platform and on a study-specific email address. The survey platform we used (Prolific) also allowed participants to rescind their participation at any point.

- **Other population-specific measures.** Finally, we tailored specific data collection and consent measures to each population. For example, for our focus groups with Syrian and Somali refugees, we had the consent forms professionally translated to Somali and Arabic, as well as hiring a professional interpreter for each focus group. I, a woman, led the focus groups, with another researcher and an interpreter, both men; case managers advised us that it would be important to have a woman researcher present as the participants were mostly women. We also prepared transportation options to the focus group site that included taxis driven by women, as case managers and teachers told us that some of the women participants traveling without men would not ride in a taxi with a male driver. For our remote interviews with activists, we kept our videos on and invited them to ask questions about us in order to build trust, but did not ask them to do the same (most chose to keep their videos off). We also invited them to review our paper before publication, and when we asked them to recruit other participants, we did so by requesting they give out our contact information to the extent they were comfortable, rather than asking them to share names.

1.3 Dissertation organization

The remainder of this dissertation is organized as follows: Chapters 2-5 present each individual research project. The introductions to each of these chapters first explore how the three themes about change and vulnerability appear in each chapter, and then I present the research itself. Chapter 6 concludes this dissertation, exploring each theme about change and vulnerability again through each project. Survey materials, interview guides, and codebooks can be found in Appendices A- C.

Chapter 2
COMPUTER SECURITY AND PRIVACY FOR REFUGEES IN THE UNITED STATES

This chapter presents my work on computer security and privacy for refugees who have moved to the United States. In order to give the reader the mindset of thinking about change and vulnerability, this chapter first explores how refugees in the US experience vulnerability to computer security and privacy harms due to the changes that they are undergoing, touching on first the nature of refugee resettlement as change, then the three themes about change and vulnerability present in this dissertation, and then turning to the research itself.

I invite the reader to refer back to Table 1.1 throughout the remainder of this chapter, which expands upon refugees, change, and vulnerability.

Refugee resettlement: a life change. Recent years have seen a number of crises around the world in which individuals flee their home countries in the hopes of ultimately resettling somewhere else. As of 2021, there were 20.4 million refugees worldwide under the United Nations' mandate, and 84,995 were resettled to the US in 2016 alone, with many fewer in later years due to policy changes [96, 97, 174, 207]. Prior work suggests that technologies play a critical role in the lives of these refugees in refugee camps, in transit, and once resettled (e.g., [92, 114, 179, 293, 326, 329]).

The process of resettling to the United States as a refugee is extremely varied. Some refugees are born in refugee camps or spend years in refugee camps (e.g., many Somalians in Da'daab refugee camp in Kenya), while others must flee on short notice (e.g., Ukrainians after the 2022 Russian invasion). Their journeys are also incredibly varied. Some receive refugee status while at home (either in a refugee camp or not) and travel with official papers to the host country, while others travel without official papers, at times with the help of smugglers and in extremely arduous or dangerous conditions, and start the process of getting refugee status only once they arrive in their chosen host country. There are also *many* people living in refugee camps who wait years or decades without being able resettle in another country due to low rates of refugee hosting by the US and many European countries. This chapter is *not* about refugees' journeys, but I provide this very brief background to help the reader understand how extraordinarily many paths there are to becoming a refugee and what their lives might have been like before coming to the US. For further reading about refugees' journeys, I strongly recommend *City of Thorns* by Ben Rawlence [237] and *The New Odyssey* by Patrick Kingsley [167]. While there are some academic works in the HCI and Security and Privacy communities about refugees' journeys, I believe this is an area ripe for future research.

Returning to the idea of resettlement and change, the minority of refugees who are invited to resettle in the US receive little support once they arrive. They are often paired with a local resettlement organization—like the one I volunteered at for years in Seattle, from which we recruited participants for the study presented in this chapter. This resettlement organization helps them apply for government benefits, knows the complexities of each government assistance program, and tries to help them become self-sufficient in the US as quickly as possible. The best way I can summarize the state of government assistance programs for refugees in the US is that the information online is complex, not all in one place, and it would be monumentally difficult to navigate this system alone. So, the local resettlement organizations are a critical part of many refugees' journeys in the US.

When refugees come to the US, it is at best like moving to a new country under good conditions, that is, it is a massive change. And, for those who spent years in refugee camps, or simply did not grow up speaking English and using technology in the same way that many do in the US, they arrive, in debt to the US government [253], knowing little to no English, in a country with a new set of cultural mores, a new language, and new technologies that they are expected to use. I will touch on these changes throughout the rest of the chapter, but I encourage the reader to keep in mind both (a) all the broad ways that moving to the

US as a refugee might be a change, and (b) the extremely varied identities of refugees (who do not all face all of the challenges I have laid out).

Theme 1: new actors, assets, risks, and technologies. Because of the massive change that comes with moving to the US, refugees encounter new actors, new assets, new risks, and new technologies when they arrive, which make it more difficult for them to maintain their security and privacy. The local resettlement agencies pair them with **case managers**—**new actors**—that the refugees may not be sure if they can trust[1]. They are pressured to attain or maintain financial stability by getting a steady job and navigating the labyrinth of government benefits (with their case manager's help), so other new institutional actors include local and federal US government offices and workers, American companies hiring workers (e.g., Amazon warehouses), and job-search websites commonly used in the US like `indeed.com` and `monster.com`.

They also have a new set of **personal information and technology.** to maintain and protect (**new assets**). I observed that **social security numbers** are a particular source of concern and confusion—a nationally identifying number that must be kept secret *or else*, except for the many instances in which organizations use one's social security number (or part of it) as an identifier. Additionally, depending on the refugee's background, some technologies may be new to them. Some may have never used a computer and keyboard before (e.g., if they grew up in a refugee camp that does not have a lot of access to computers); others may fluently use smartphones and computers but may not use email regularly or at all.

Refugees also encounter **new risks** in the US. At a high level, they are not as intimately familiar with **US laws and customs** as people who grew up in the US, so they may be unsure how to threat model about, for example, minor traffic violations (as shows up in our study in Section 2.5.1.3). Some—especially those who have not received the official refugee status and are instead asylum seekers—are concerned about US immigration laws,

[1] I have every reason to believe the case managers I worked with, and all of the ones in this study, are genuine and trustworthy people, but I am considering the the refugee's threat model here.

xenophobia, and racism.[2] Some may also be experiencing **scam and phishing attempts** for the first time in the US and, in combination with new assets, new technologies, and new actors, may not be confident in identifying scam attempts.

Theme 2: a changed prioritization of digital security and privacy. The second theme in this dissertation is about *changing prioritizations* of security and privacy, which appears in this chapter as idea that **refugees may prioritize other needs, e.g., financial security, over security and privacy**. Participants told us that refugees, having been told not to give away their social security number, check with case managers before entering it into a job search website, and may not be entirely comfortable entering it even when the case manager gives their approval. They also may be reluctant to share their social security number, or other information that can be sensitive, with case managers or other people acting in official capacities (Section 2.5.2).

Additionally, some information may be out of the refugees' control. For example, many of the case managers actually check their clients' email accounts for job search emails, but this means that the case managers have complete control over the email account and credentials. Some refugees have email accounts specifically for the job search, while others mix personal and job search, but either way, they do not have sole control over either the email account that contains information about their job search, including highly personal and identifying information, nor the storage of their credentials. So, this is an example of how **refugees are at times *unable* to prioritize security and privacy** even if they want to.

Theme 3: technology design exacerbating existing systemic discrimination inequities. To build on the example in the previous theme, about case managers managing clients' email addresses—my point is not about how exactly case managers store the credentials, or whether or not this is a "good" security practice. My point is that technology does

[2] In our study, at least one participant brought this up, but we did not have space to include it in the original paper.

not support this use case happening securely and privately, and that general-purpose security advice about (not) sharing passwords does not work for this relationship. More broadly, I found that **cultural assumptions misaligned with the backgrounds of many refugees were pervasive throughout the technology they use** and, furthermore, that they were highly incentivized or forced to use this technology by the pressure to become self sufficient. So, throughout the following chapter, note how (a) these cultural misalignments contribute to the increased workload necessary to maintain security and privacy for refugees, and (b) societal systems force refugees to use these technologies in the first place.

For example, refugees are under extraordinary pressure to search for a job almost as soon as they arrive. Many companies use or require online applications and communicate with applicants over email. However, at least at the time of our study in 2018, GMail's email account creation process requires users to answer security questions that may be incompatible with people who might not change names due to religious or cultural reasons, or people who are not comfortable using a keyboard and mouse and thus may be confused by typing in a password in a hidden field, or who may create a password without capital letters. **Though each of these practices are not themselves insurmountable**—e.g., a Muslim user (or any user) could (and should?) enter an answer other their actual mother's actual maiden name—**they contribute to a system of privileges that favors users from western, educated, industrialized, rich, and democratic (WEIRD) backgrounds in a country where sociopolitical systems already favor those users**.

Co-authors and original publication. The remainder of this chapter was originally published at the IEEE 2018 Symposium on Security and Privacy [271]. In this chapter, I use "we" to represent the work and writing done by coauthors Ada Lerner, Samia Ibtasam, Franziska Roesner, and Tadayoshi Kohno (in the order that they appear on the published paper). I have made minor adjustments to the tables and text, including moving some of the original introduction text to this section.

2.1 Introduction

Our research is driven by the following questions: To what degree must refugees, once resettled, depend on technology in their efforts to integrate into their new societies and reestablish their lives? On which technologies do refugees depend, and how could they be harmed if they are unable to adequately secure their digital footprint? What computer security and privacy practices do refugees have, and what barriers do they face that prevent them from implementing stronger security and privacy practices? And, perhaps most importantly, what could be done to empower refugees with greater capabilities to protect their computer security and privacy?

We hypothesize that refugees—a vulnerable population according to the United Nations High Commissioner for Refugees (UNHCR) [97]—may be different from other user populations in terms of their interactions with technology and their computer security needs and practices. Refugees, by definition, are fleeing from real threats, and hence might have unique perspectives on threats and adversaries. Further, there might be a range of cultural, linguistic, and technological challenges that refugees must overcome in order to sufficiently protect their computer security and privacy.

Thus, in this work we study the computer security and privacy needs, practices, and challenges among refugees—specifically, refugees from East Africa and the Middle East who resettle to the United States. While we believe that the inquiry into this population and our results are of scientific interest, we also believe that our work can provide a foundation for helping refugees have a secure and private digital presence.

Methodology Overview Refugees around the world are a large and heterogeneous population. We study specifically Middle Eastern and East African refugees in the United States—allowing us to both focus our efforts and dive deeply into the concerns of these populations, while still considering refugees from a variety of backgrounds. We conducted semi-structured qualitative interviews and focus groups to broadly explore the computer security and privacy challenges, needs, and opportunities for this population. As is common for formative studies of this type [45, 122], we focused in-depth on a small number of participants.

Through initial contact with an NGO committed to assisting refugees and immigrants, we learned that arriving refugees are assigned case managers (who help their assigned refugees find jobs and otherwise matriculate into society) and English teachers. Both case managers and teachers play a central role in the lives of refugees, and they often introduce refugees to or help them with technologies necessary for their lives in the US (e.g., setting up an email account to communicate with potential employers). Similar to other work studying resettled refugees [19, 29], we conducted interviews with case managers and teachers because of the broad perspective they have across the many refugees they work with, and because refugees themselves are a potentially vulnerable population. We interviewed four teachers and five case managers, four of whom were refugees themselves.

We then used the results of the interviews with case managers and teachers to help guide our direct interactions with refugees, which complemented and corroborated the interviews with case managers and teachers. At the suggestion of a case manager, rather than interview refugees individually, we conducted several small focus groups, where each focus group had participants who fled from the same country (Syria or Somalia), and the discussions largely took place through an interpreter. Our use of focus groups, rather than one-on-one interviews, enabled free-flowing conversations with the refugees, and in less intimidating settings than one-on-one interviews. In total, we conducted three focus groups, one with four Syrian refugees and two with five Somali refugees each.

Foundations for Refugee Computer Security Our interview and focus group results shed light on the computer security and privacy needs of the refugee population we study, as well as the unique barriers they face to protecting their digital security and privacy. Example themes that emerged include:

- Consistent with our hypotheses, we find that refugees today *are* highly dependent on technology in order to establish themselves in the US. However, we did not anticipate just *how* dependent on technologies they are. Whether to apply for jobs, or to find housing, it is impossible for them to escape the need to use technology. This reliance on technology makes computer security both critical as well as (in some cases) in tension with other, primary goals (such as finding a job).

- When refugees enter the US, they must learn not only how to use technology, but must also overcome language and cultural barriers. Critically, we find that many computer security and privacy related practices include deeply embedded US or Western cultural knowledge and norms, including the use of birth dates as authenticators and common techniques for creating memorable passwords. Indeed, the very notion of a scam seems foreign to some refugees.

- We know, from our preliminary conversations with a local NGO focused on refugee and immigrant support, that case managers play a central role in helping refugees establish themselves in the US. However, we did not anticipate the extent to which refugees must trust their case managers, even when in some cases they do not want to trust them. The computer security practices of refugees are thus intimately tied to the security practices of their case managers, and their relationships with them.

From these and other findings, we make concrete recommendations to bridge gaps we observe in how refugees are able to protect their digital security and privacy—for example, to support more secure use of public computers or account management solutions that explicitly support access by trusted parties like case managers.

Ultimately, by providing a broad basis for understanding how recently resettled Middle Eastern and East African refugees in the US interact with technology, our work provides a foundation for future, deep-dive investigations into specific technical needs, which may also apply more broadly to other groups sharing some of the same characteristics.

2.2 Background on Refugees

The processes surrounding how people become, and how countries accept, refugees are complicated. We provide essential background about refugees and the refugee process here, focused on—given the scope of our study—refugees who resettle in the US.

Definition of a Refugee Refugees are people who have left their home country due to a "well-founded fear of being persecuted for reasons of race, religion, nationality, membership of a particular social group or political opinion" [4]. In 2016, there were an estimated 22.5 million refugees worldwide, and an additional 2.8 million asylum-seekers (people who want refugee status but have not received it yet) [207].

Resettlement Process Before arriving in the US, refugees must pass extensive background checks and interviews. Refugees will, in many cases, have also spent years in intermediate countries or refugee camps before arriving in the US [97]. Before resettling, refugees attend a cultural orientation, which provides a breadth of information about the US.

Aid after Resettlement, Case Managers, and Teachers The US State Department assigns each refugee to one of nine national resettlement agencies [97]. To assist in their transition, refugees are also paired with local NGOs, like the one we recruited from. The NGO we recruited from, and others, assigns refugees *case managers* and offers English classes. Case managers refer to their assigned refugees as *clients*, a term that we will also use interchangeably. Case managers, who may be refugees themselves, can have diverse responsibilities, but in general those responsibilities include helping their assigned refugees (clients) find jobs and otherwise matriculate into the US [95]. Case managers typically speak their clients' native language. The English classes are taught by English as a Second Language (ESL) *teachers* and are intended to help refugees communicate in their new environment.

2.3 Motivation and Research Goals

There is a growing body of work considering diverse populations in computer security literature, with recent studies focused on specific potentially vulnerable user groups, including low-income people in the US [189], domestic abuse victims [99, 195], and journalists [198]. Refugees are a population with unique backgrounds (e.g., fleeing threats in other countries) and constraints (e.g., at least initially, lack of familiarity with the English language, and highly dependent on the US government and NGOs for support).

Our ultimate goal is to help refugees protect themselves from computer security and privacy threats. To address this goal, however, we cannot blindly set out to design and build security tools, or develop security education campaigns, intended for refugees. First, we must deeply understand the world in which resettled refugees operate, and how they interface with technology. We use interviews and focus groups to form this deep foundation (Section 2.4).

For our interviews and focus groups, we do not want to presuppose that refugees should use technology, or, if they use technologies, that the so-called security best practices for most users are the optimal security best practices for refugees. This perspective—both valuing security, but not wanting to assume that *our* views of security will match the views of refugees—guides us to formulate the following specific research questions for our interviews and focus groups:

1. How do refugees use technology as they settle in the US, if at all, and how might their relationships and life goals influence that use?

2. What barriers inhibit the implementation of strong security and privacy practices among refugees?

3. What computer security and privacy practices do refugees have?

4. What do refugees learn (e.g., from case managers and teachers) about computer security and privacy?

Participant Description	#	Avg Years in Job (Range)
ESL teachers	4	1.9y (0.5y - 3y)
Case managers	5	2.4y (0.4y - 5y)

Participant Description	#	Avg Years in US (Range)
Syrian refugees	4	0.5y (0.4y - 0.6y)
Somali refugees	10	8.1y (2y - 18y)

Table 2.1: Summary of all participants.

These research questions are intentionally broad and exploratory, enabling us to step back, ask, and answer higher-level questions, such as: Are refugees exposing themselves to unnecessary computer security and privacy risks? If they are, is it due to a lack of awareness, a language barrier, a lack of education, or something else? Is conventional wisdom about computer security best practices sufficient to enable secure practices for refugees, or are unique solutions needed? And, if there are any shortcomings, what could be done by the computer security and privacy community to empower refugees with greater computer security and privacy?

2.4 Methodology

We use semi-structured interviews with case managers and teachers and focus groups with refugees to answer the research questions outlined in Section 2.3. We conducted interviews and focus groups between May and September of 2017. All our activities were approved by our institution's IRB, and we discuss human subjects ethics further below. Table 2.1 summarizes our participants.

Semi-structured interviews with case managers and teachers We conducted semi-structured interviews with four ESL teachers (T1-4) and five case managers (CM1-5) from a local NGO that provides support to refugees and immigrants. Each interview was conducted by two interviewers, and all but one of the interviews were audio recorded and transcribed for later data analysis. One case manager interview was not audio recorded because the interviewee did not wish to be recorded; one interviewer took detailed notes, which served as the basis for that interview's later data analysis. Interviews were conducted in English, in which all participants were fluent, and lasted 1-2 hours. We conducted interviews until reaching thematic saturation, and then turned to focus groups of refugees to corroborate and complement the teachers' and case managers' perspectives.

By asking teachers and case managers for their observations of their clients, we elicited a broad view of refugees' technology usage and threat models: case managers had between 42 and 50 clients, and class size for teachers varied from 12 to 34 clients. After accounting for the overlap between teachers and different case managers, we conservatively estimate that we talked about approximately 150 refugees from 22 countries, with the most common countries being Eritrea, Ethiopia, Iraq, Somalia, and Syria. Since the case managers and teachers drew on many years of experience, they likely drew their answers from experiences with a far greater number of refugees. Additionally, four of the five case managers were themselves refugees, and provide personal insight into refugees' views as well as a high level view of their clients'.

Driven by the research questions in Section 2.3, each interview covered the following broad topics: technology usage, threat models, and technology education. We asked about each of these topics in the context of both refugees' lives currently in the US and—to develop an understanding of why refugees might have whatever practices and beliefs they currently have—we asked about each of these topics in the context of their lives prior to the US, including time spent in refugee camps, home countries, and any intermediary countries. We waited for participants to bring up security and privacy organically; if they did not, we brought it up about halfway into the interview.

We note that case managers' and ESL teachers' view of refugees may be skewed towards those who do not yet have jobs, or who do not have the technological or English skills to independently get a job yet; therefore our results are biased to apply more strongly to the population of refugees with weaker English and technology skills. However, this sub-population—refugees who do not have jobs or are not fluent with technology—is a critical population to assist.

Focus groups with refugees To complement the case managers' and teachers' interviews, we conducted three focus groups with refugees. All focus groups had two researchers and a professional interpreter, and the focus groups were audio recorded and transcribed for later data analysis. We chose to use focus groups with the refugees, instead of semi-structured one-on-one interviews, because focus groups—unlike interviews—would allow refugees the opportunity for free-flowing conversations amongst themselves, and because we wanted to create a non-intimidating environment where the refugees could follow the norms of their peer group regarding what to share.

The first focus group was with four Syrian refugees (R1a-d), and the second and third groups were each with five Somali refugees (R2a-e, R3a-e). To facilitate discussions, we asked participants to arrive in groups with whom they were already comfortable (e.g., families or friends). However, asking participants to arrive in groups resulted in a lack of diversity. For example, the Somali subjects spanned multiple generations, but all ten were female, commensurate with most case managers' and teachers' observations that most of their clients were female (T1, T3, CM1, CM2, CM3, CM4).

Interviewing Syrians and Somalis allowed us to speak to refugees who represented the majority of the clients that the case managers and teachers were discussing.

Data analysis To categorize and coalesce the data from our interviews, we iteratively developed a codebook with hierarchical descriptive codes through several rounds of coding, first using open codes, and then combining them to create axial codes. Each interview was then coded by two members of the research team, one of whom coded every interview (the primary coder). Intercoder agreement was high: using Cohen's Kappa, a standard measure for two coders, our average intercoder agreement was .98. When we report raw numbers here, we use numbers based on the primary coder's codes in the case of (rare) disagreement between coders.

For the focus groups, when reporting on the number of people who mention a topic, the reported numbers will be lower bounds on the views of the participants since, if one participant says something and another agrees, that second participant may not say anything. Additionally, because each audio recording reflected multiple voices, particularly when refugees had a discussion in their native language which was then summarized by the interpreter, it is in some cases difficult to attribute individual comments to specific participants. Instead of coding for each refugee, the researchers developed a consensus on all themes across the full group and, when reported on here, worked to attribute specific statements to individual participants.

Human subjects and ethics Our entire study protocol was approved by our institution's IRB. Because we were working with a vulnerable population, we took care to design our study to protect participants' privacy and treat our subjects ethically. We did not unnecessarily collect personally identifying information, we asked participants to anonymize names in their own stories, and we redacted names and other personal details in our transcripts. With explicit consent, we audio recorded all interviews except for one, because the participant was not comfortable with it.

In developing the interview and focus group protocols, we focused on technology use as much as possible and avoided asking about potentially sensitive or emotionally difficult topics. Participants were explicitly not required to answer questions (and some exercised the option not to answer).

In presenting our results, we do not name the NGO from which we drew participants, and we omit some details (such as gender) so that they cannot identify each other.

2.5 Results

We now turn to the results from our interviews with case managers and teachers, as well as our focus groups with refugees. We organize our results around the four core research questions raised in Section 2.3: (1) How do refugees use technology as they settle in the US, and how might their relationships and life goals influence that use (Section 2.5.1), (2) What barriers inhibit the implementation of strong security and privacy practices among refugees

(Section 2.5.2), (3) What computer security and privacy practices do refugees have (Section 2.5.3), and (4) What do refugees learn (e.g., from case managers and teachers) about computer security and privacy (Section 2.5.4).

2.5.1 Refugees and Technology

We begin by considering the technologies that refugees use (Section 2.5.1.1), their relationships with case managers and teachers (Section 2.5.1.2) and others in their community (Section 2.5.1.3), and their life goals (Section 2.5.1.4). These findings provide context for later subsections, in which we also consider how those relationships and goals might interface with their technology use and computer security behaviors.

Some results, such as those about technology use, may apply to groups beyond refugees, such as non-refugee immigrants from the same regions. Other results, such as those about refugees' relationships with their case managers and teachers, are more specific to refugees. Future work could explore these issues more deeply, to better understand which issues are inherent to refugees, and which issues are faced by other groups.

2.5.1.1 Technology Use

Overall, we find that there is a dichotomy between refugees who are fluent using technology, and refugees who are not. Over both groups, prior email usage is low. Despite the diversity in technical and educational backgrounds, the goals for their lives are similar now that they are in the US.

Experience with technology prior to the US T4 and CM3 observed a clear division between refugees who use phones and computers fluently, and refugees who are much less tech literate. The first group is typically refugees from cities who are comfortable with technology, smartphones, computers, have social media, and are well-versed in messaging and VoIP apps but still may not have experience with email (CM3). These refugees are likely to be from wealthier countries like Syria or Iraq, and some from larger cities in Ethiopia (CM1, CM3).

In contrast, refugees who grew up in rural areas or spent many years in refugee camps have little to no experience with technology. Some have never used a computer or a mouse before: "*Somebody that comes from a refugee camp... you have to explain to them what e-mail is, what does it do for you? How do you communicate with people that you don't see, but you're still talking, e-mail. What kind of information should I share with them?*" (CM3). This quote also points to circular issues around teaching email and information security and privacy to refugees whose mental models of computers and the internet are not well-developed.

While some refugees have not used a computer before, many do arrive in the US familiar with smartphones (T3, T4, CM2, CM3). In both groups, refugees were unlikely to have email addresses; instead, refugees with more technical experience used apps like WhatsApp and Viber (CM2).

The majority of refugees that the teachers and case managers spoke about were in the latter group—uncomfortable using computers, and with a varying amount of smartphone experience. Refugees in the focus groups were more technologically proficient. We hypothesize that this difference is due to the country of origin for the first group (Syria), and the length of time in the US for the second and third groups (Somalia). (Table 2.1 summarizes these demographics.) This supports the case managers' and teachers' view of Syrians having more experience with computers, and shows that refugees who may enter with less tech fluency, such as Somalis, go on to incorporate technology in their daily lives after living in the US for years—suggesting that teaching computer security and privacy practices is critical early on.

Tech use in the US: Computers Teachers and case managers said their clients typically do not have computers at home (except some Iraqi and Syrian families). Thus, the majority of their computer usage is on public or shared computers, e.g., at a library, a community center, or in a computer room in a local NGO (T1, T2, T3, T4, CM2, CM4). Refugees use these shared computers for job searches and job applications, raising potential security

Common Smartphone Uses	**Participants**
Connecting with friends/family	
Messaging	T*, CM*, R2{bde}, R3{ab}
Social media	T*, CM{135}, R1{ab}, R2e, R3{cde}
General everyday use	
Navigation	T{124}, CM{125}
Translation	T{124}, CM{35}
Photos of important documents	T2, CM{123}, R1a
Other	
Email	T*, CM*, R1{cd}, R2{bce}, R3b
Watching videos	T{24}, CM1

Table 2.2: Current smartphone use by refugees. Notation: T{24} denotes participants T2 and T4; CM* means all case managers (CMs).

concerns for their personal information due to the shared nature of public computers. These practices have implications for both the administrators of the machines and teachers and case managers who are teaching computer etiquette and security.

Tech use in the US: Smartphones All teachers and case managers said that most if not all of their clients have smartphones; all the refugees in our focus groups had smartphones. Because many refugees own smartphones, but *not* computers, it is important to understand that their smartphones are the connection to their digital lives.

Table 2.2 shows the most common smartphone uses, including connecting with family and friends abroad via WhatsApp, Viber, and Facebook (among other platforms): *"I like to use Facebook to communicate with my parents and my family members back home... If the apps were not there, I would have to buy phone cards and call people overseas, but now because of the technology and the apps, it's easier for me to communicate without purchasing* *those phone cards"* (R3c). They also use smartphones for everyday tasks like navigation, translation, and storing photos of important documents, a practice that we will return to in Section 2.5.3.

Notably, we have put "email" in the "other" category in Table 2.2, since teachers and case managers told us that a main use of email for refugees is to contact potential and current employers (T4, CM2, CM4, CM5), and, depending on the refugee's English level, they may wait for their case manager to help respond (CM3). Although one case manager observed that refugees may also get personal emails, this case manager was adamant that case managers should ignore those emails when accessing a clients' account to help with job-related activities (CM5); we return to a deeper discussion of email use in Section 2.5.3.

2.5.1.2 Role of Case Managers and Teachers

Refugees must trust their teachers and case managers in order to leverage their knowledge and services, but this also puts them at risk, since in doing so they must trust the security measures of every person or organization they give their information to. While case managers and teachers gave us every reason to think they were trustworthy, there is always the potential for mistakes or for a malicious insider—making this requirement to give out information a significant and unavoidable potential vulnerability for refugees.

Case managers help refugees settle into their lives in the US; the main responsibility of the case managers we interviewed was helping their clients find a job. Because their employer (the NGO) requires it, case managers must collect sensitive and personal information from clients such as photocopies of their social security card and first paycheck, but are required to adhere to strict confidentiality agreements (CM1, CM2).

Teachers and case managers indicated that they trust their colleagues completely, and that their clients should as well. However, T2 said that refugees sometimes do not trust their case managers with their personal information; T2 attributed this to trauma from their past. "*It's not every day, it's kind of like a wave, where one day they're totally fine with their case manager and the next day it's like, 'I don't know this person, I don't trust them.'*"

This causes problems for both refugees and case managers because refugees have to share sensitive information with their case managers in order to get the case manager's help. This trust relationship with teachers and case managers extends to trust in the digital domain, a topic we return to in Section 2.5.3.

Teachers do not have as much interaction with clients that revolves around their own personal information. At the NGO we recruited from, the ESL curriculum covers practical English skills (T2). Some ESL teachers devote a small amount of time per week or month to teaching computer skills, such as typing, logging onto email, and clicking on links (T1, T3, T4). ESL classes can also include discussions about security, like how to avoid scams or how to understand if a news source is reliable, but security is *not* the main goal of the class. Nevertheless teachers report that refugees do share with them their passwords, so that the teachers can help them log into their email accounts (T2, T3). This act raises questions of refugee autonomy when interacting with computers, as well as the question of who else they must share their passwords with in order to achieve their computing objectives.

Case managers and teachers reported that refugees had complete trust for teachers; T2 suggested that "*because I have a relationship with the students on a day-to-day basis, they trust me maybe more so than they trust their case managers.*"

2.5.1.3 Role of the Community

Newly resettled refugees find communities of others from their country who speak their language. These communities are a major source of cultural and security knowledge. R3a said she heard of scams from her community, but only after it was too late and she had already been scammed. This situation speaks both to the role of communities in sharing security-related knowledge, and the fact that scams may be an unknown concept to refugees.

In addition to explicit security advice, participants told us that that refugees receive advice about American culture and "official" offenses. CM2 said that relatives, friends, and people in the community "*will tell you, 'Okay, never make any mistake with parking or traffic accidents,' or anything like that. Never have any illegal things. Immediately they will try to* *scare you or train you mentally like that.*"

Both these examples speak to the broader observations that refugees form their security practices in part from the advice of others in their communities, in addition to advice from their case managers, teachers, and official resettlement orientations.

2.5.1.4 Refugee Goals in the US

Finally, we provide additional context about refugees' broader goals once they arrive in the US. Understanding these goals is critical to our efforts to understand and improve computer security and privacy for this population, since, as we discuss further below, commonly recommended security practices can be in tension with these core goals.

- *Establish their lives in the US.* Teachers and case managers expressed that the foremost concern for refugees is reestablishing their lives: obtaining housing and, most of all, getting a job (T1, T2, CM3, CM4, CM5). Achieving these goals requires navigating web pages filled with jargon, filling out online forms, and sending emails to various agencies and companies.

- *Keep in touch with family and friends.* Refugees' families and friends are often scattered around the world. Participants often described refugees' use of messaging apps or social media in the context of exchanging news with distant friends and family (T2, T3, T4, CM2, CM3, CM5, R1ab, R3ce).

- *Learn US culture and English.* Refugees need a working knowledge of English to thrive in a job, so they attend ESL class four times a week to learn English. Sometimes, T3 speculated, their desire to learn English and US culture leads them to be insufficiently skeptical of people speaking English. We also observe throughout our results that both technical *and* US cultural knowledge are needed for many common security features.

- *Increase technology use.* Although teachers and case managers said that they sometimes had to pressure their clients to use technology (T2, T3, CM3, CM4), we also heard about clients who were excited about using email and the internet to connect with faraway friends and family (T2, T3, T4, CM1). "*For students who understand it, it's really exciting because it's a new way to connect with the world. They'll get a new email address and they'll be like, 'I hear my brother has an email,' and we're like, 'Yeah, you can write your brother now.'*" (T4). With increased proficiency on the computer, refugees can apply for jobs by themselves, but may also increase their risk to computer security threats.

2.5.2 Refugee Security Barriers

Given the above context, we now turn to our second core research question: what barriers inhibit the implementation of strong security and privacy practices among refugees?

Past Experiences: Trauma Many refugees feared surveillance and government-perpetrated violence in their home countries. Among our study population, the countries about which we heard concerns expressed included Eritrea, Syria, and Iraq; by contrast, we heard that there were not such concerns in Somalia (CM2, R3c).

Case managers identified a fundamental difference with "*[those who] were born in, for example, a stabilized country, they are different than people who come from a war, who are suppressed*," (CM5) such as those from Eritrea, Syria, and Iraq. CM5 said that in Iraq, "*the walls have ears*," meaning that anyone, even the neighbors, could be reporting back to the government. "*You never know who's listening and you could be killed for it, you could disappear overnight for it*" (CM3).

CM2 drew a distinction between Somali clients, who "*talk [about] anything they want*" and Eritrean clients, who "*you never see... talking about the government or anything like that.*" Compared to a country with censorship, CM1 explained, "*in Eritrea... you can use [any website]. There is not any problem. The problem is on what things you are writing or you are speaking.*" T2 and CM4 additionally identified trauma from the past as an irrational but unavoidable factor in refugees' decisions to trust certain people or entities. As we discuss in Section 2.5.3, refugees must trust people—such as their case managers—for assistance, when establishing themselves in the US.

Language: Dependence on Assistance Refugees face linguistic barriers (T1, T2, T3, T4, CM2, CM3, CM5), increasing their reliance on others for help with tasks that must be completed in English, like a job or housing application. The impact of this language barrier manifests in multiple ways, ranging from email account management, to website validity verification, to scam avoidance.

Culture: Awareness of Risks We also found that while certain types of security risks are well-known within US culture, they are new concepts to many refugees. Consider, for example, scams and identity theft. From our interviews, we observed that a concern for identity theft and scams was typically instilled by case managers, teachers, or others over time, or through direct experiences (e.g., R3a was scammed twice before learning to be cautious), rather than a concern refugees brought with them from their home countries. Case managers and teachers suggested that refugees were surprised by the possibility of such threats: "*They always ask me why. 'Why would they do that? Why would they take my social security?' ... They're surprised that [on] this side of the world, somebody will go through all this hassle just to destroy somebody's identity or life*" (CM3). T3 remarked, "*I don't think they have the idea that there might be something that could be potentially risky for them in their inbox*" (T3). CM4 suggested that the novelty of these types of threats may cause refugees to treat their personal information with insufficient caution: "*Imagine someone who has no exposure or little knowledge about computer hacking.*[3] *They can't believe, and they can simply provide all information.*"

Case managers emphasized that there *are* refugees who are already skeptical of putting their information on the internet (though they may be a minority), such as the participants

[3] In this case, CM4—not a technical expert—used the term "computer hacking" generically to include attackers like scammers.

in R3, who together listed identity theft, catfishing, being taken advantage of by a trafficker, and having their locations tracked through the use of various apps on their phones: *"the internet has benefits as well as risks"* (R3a). We further discuss perceived threats like these in Section 2.5.3.5.

Culture: Exploiting Barriers Our interviews surfaced the fact that refugees' lack of awareness of risks, and their dependence on assistance, make them particularly vulnerable to scams. For example, we heard anecdotes about scam websites and phone calls asking for information for a (fake) low-income housing application, ads for (fake) minimum-wage jobs, (scam) phone calls about utility bills being overdue or arrest warrants, or tax scams around tax day (T2, T3, T4, CM4). Refugees—particularly recent arrivals—are only just learning the US bureaucratic processes, as they do not have experience living in the US, paying US taxes, or applying for jobs in the US, and hence can have a particularly difficult job distinguishing a legitimate request from a fake request. Indeed, T5 observed that when someone calls a new refugee on the phone, and speaks to them in English, they assume that the person must be someone of authority who is there to help them.

Culture: Secrecy and Sharing of Information Case managers and teachers said that refugees from some areas, particularly more rural areas, have a different set of personal information, and may share that information more or less freely than is commonly expected in US culture. For example, in some cultures birthdays are not awarded the same significance they are in mainstream US, so when refugees arrive from these cultures and do not know their actual date of birth, they are assigned a birthday of January 1. Even with refugees whose children do have officially documented birthdays, the parents may have difficulty remembering the precise day: "*You know, when they come here, the last thing they want is to remember ... if you have, especially seven, eight kids, to remember, each one of them, the day the month and the year. 'Cause you worried about getting them housing, and you worried about food stamp doesn't get cut, worried about getting the work, and just standing* *on your feet. The last thing you want to know is who was born in July, who was born in December.*"

Security mechanisms that rely on a high-entropy distribution of birthdays will not be as secure for refugees from these cultures (i.e., East Africa, but *not* Syria); relatedly, other security mechanisms or common password generation algorithms may use other information, such as the personal information of close family members, which may be shared to a different set of people. R3a, from Somalia, expressed concern that matching birthdays and other information like name with someone else could cause issues: *"You will find someone with the exact same birthdate, name, whatever, the only difference is the address. And maybe this person did something ... and now ... [the government] just hold your identity on hold, and maybe travel, like traveling out of the country, and someone with same information as you has been flagged to travel out of the country ... And if you need to cross the border, to another country, that name is going to pop out because it is flagged. And you matched with them so you're going to have to go through the questions to identify if this is the official person or not."*

Technical: Lack of Experience As Section 2.5.1.1 observed, refugees can have varying degrees of experience—some have had prior technology experience, whereas other do not have experience with computers or keyboards. And, as noted above, email is a new concept to many refugees, even those with prior technical experience. When encountering a new technology, refugees naturally focus on the primary goal of trying to learn how to use that technology to accomplish a task (e.g., read email, or use YouTube to learn English), rather than how to use it securely and privately.

2.5.3 Refugee Security Practices

We now turn to our analysis of the security and privacy practices that refugees have. One salient observation we have is that computer security is *not a priority* for refugees, due to a combination of the barriers they face: for example, if initially they do not know about scamming, they do not prioritize securing themselves and their assets against scammers. But, even when they are well aware of scamming as a threat, they may not be *able* to prioritize security against scammers, for multiple reasons: (1) even if they want to prioritize security goals, they may not have the technical knowledge to do so, and (2) other goals under the umbrella of establishing their lives in the US, such as going to appointments or getting jobs, may take priority over security.

2.5.3.1 Online Authentication

We find that refugees face significant hurdles with online authentication. These challenges cause them to rely on their case managers and teachers for help with account creation and access, particularly in the case of email accounts (which refugees need in order to obtain many jobs). Broadly, these challenges indicate that text-based passwords and security questions do not allow refugees' accounts strong security because of the barriers that refugees face in implementing them.

While case managers and teachers focused their discussions on email account creation and access, since that fell under the scope of their jobs, many of the issues raised below apply to authentication in general.

Password Creation One initial challenge refugees encounter when trying to create email accounts—and likely other accounts as well—is password creation. There are two key challenges with password creation for refugees: the privacy of passwords and the entropy of passwords.

For email accounts, case managers frequently help create usernames and passwords for their clients. In doing so, some case managers rely on password creation strategies that scale for their purposes but are "*not... unguessable*" (T2), including simple algorithms based on personal information about the client (for some case managers) as well as the same password for all their clients (for other case managers).

While there are natural security concerns with having someone else pick passwords for refugees, T3 also expressed concern about refugees picking their own passwords: "*They need to be a little more careful of passwords... if they don't do that very generic password [set by their case manager], they will pick their child's name, the year they were born, something like that, that they can remember easily.*" Indeed, this practice is confirmed by R1a, when discussing how to pick a password: "*As much as I know, lots of people use their birthdays, but it doesn't mean they put it in a proper way. They put the birthday, but they make some changes in it. Maybe we add a star or a zero or something extra.*"

Password Memory Case managers and teachers commonly identified forgotten passwords as an issue (T1, T2, T3, T4, CM1, CM2, CM3, CM5, R1a). CM3 attributed this partly to a cultural and language barrier: "*So, the last thing they want to remember is numbers, passwords, usernames, all this new to them. And add to that, is a different language. So it's a really a challenge.*" Typically, the case manager or teacher helps the client recover the password, either by setting a new one, or, in some cases, by logging in with the real password that the case manager or teacher has saved. In extreme cases, clients lose access to their email accounts permanently if they forget the password, recovery phone number, recovery email address, or security question answers (T4).

Password Entry Even when refugees know and remember their own passwords and security question answers, typing them correctly can present difficulties for refugees with limited prior experience with computers (CM2, CM5, T2, T3, T4). T3 said that capitalizing letters, i.e., with the shift or caps lock key, is sometimes difficult, especially if the password is not visible. Attempting to avoid this challenge may result in refugees creating weaker passwords (e.g., using only one character set).

Security Questions Though security questions for account recovery provide questionable security [261], they are nevertheless common. However, we find that security questions are designed with implicit US cultural knowledge and norms embedded—sometimes making these questions inapplicable to refugees. For example, questions about a mother's maiden name are not useful for people from cultures in which women do not take their husband's name (T4). Other questions are difficult or impossible for people with limited English skills or who did not grow up in the US: some refugees have never gone to school or owned a car, and small villages in East Africa, for example, may not have street names. Similarly, some questions may ask about information that is typically private in the US but common knowledge in other cultures (e.g., family or childhood details), or may ask about information not considered important or distinct (e.g., birthdates). As a result, refugees' responses to security questions may be insecure or easily forgotten: "*For a newcomer, they might not be used to keeping that kind of information in their heads, so I think that they might make up answers and then forget, or forget what the question was asking*" (T4).

2.5.3.2 Email Account Management

Since a primary goal of case managers is to help their clients find jobs, and since email access is critical to refugees' job search, we now turn more deeply to the relationship between case managers and their clients' email.

Case managers and teachers often become primary users of these accounts, maintaining credentials as well as reading and responding to job-related emails on behalf of their clients. This practice (particularly when a refugee also uses that email account for personal purposes) trades off potential vulnerabilities with the critical utility of an email account as part of the job search process. In short, refugees rely heavily on their case managers and teachers for help with email use and account management, which means that refugees must trust their case managers significantly.

Password Management Across Refugees In order to efficiently check 40-50 clients' emails every day, and to help clients in the (frequent) cases where they forget their passwords, case managers have developed certain password management strategies to streamline their process. Three case managers keep spreadsheets with all their clients' email usernames and passwords, and another case manager keeps the credentials "*on a paper in the [client's] file,*" which "*gets locked up every day.*" One of the case managers who keeps a spreadsheet also uses the same password for all clients for whom they create a password. Likewise, teachers keep copies of clients' email credentials to help with email account access and recovering from forgotten passwords.

These password management strategies—including storing and reusing passwords—do not conform to many common password "best practices" and are vulnerable to certain classes of attackers. However, these strategies reflect the tensions inherent in the time constraints and main goals of case managers and teachers: to efficiently and effectively help refugees find jobs. Thus, for case manager and teachers, the benefits of insisting on more secure password strategies may be outweighed by the benefits of efficiently logging in to their clients' email accounts.

Email Content Access Because case managers and teachers often have access to their clients' email accounts, the contents of these accounts are not private, and are also subject to the security and privacy decisions of the teachers and case managers. CM5 mentioned seeing clients' personal emails, but ignores them out of respect for the client's privacy: "*when I check emails... they're sometimes sent from friends, back home. I don't care about them. I look for ones that are job related. I can tell when they are personal. Sometimes the emails are in [their native language, which CM5 fluently speaks], so I can tell it's from a friend or relative.*" Though CM5 ignores these emails, this speaks to the power that case managers and teachers have to access these accounts.

2.5.3.3 Web Site Legitimacy

Earlier we note that teachers and case managers try to help clients understand the importance of protecting against scams and identity theft. But even if refugees know it is important, teachers and case managers said that many of their clients lack the technical experience to protect themselves online and with their digital assets. Teachers and case managers felt that their clients need to be more careful giving out information online (T1, T2, T3, CM2 CM3) and indicated that their clients often do not look for technical clues of illegitimate websites, like inspecting URLs or domains (T2, T3, CM3, CM4).

Although case managers and teachers generally did not observe refugees directly inspecting URLs to judge the legitimately of websites, refugees do sometimes employ strategies to ensure that they only visit trusted websites. For example, R3c discussed only visiting websites that she already knows, and CM1 advises their clients to only trust websites printed on a job application or a business card. Over the course of our interviews, standard security measures—like HTTPS or browser phishing warnings—did not come up.

We also find that refugees commonly turn to their teachers and case managers for help determining whether a website is legitimate. CM1 recounts: "*Most of [the] clients, they don't want to put their private things on the internet, they don't trust that much. They are new, they say, 'oh, is it okay to put in this, I try to apply this job on this website, is it proper to put my social security here?'*"

However, other case managers and teachers observed that caution with website identity was rare. For example, T3 was happily surprised to see that some of their clients did not fill out their social security number on a job application, but emphasized that they were a minority.

Even those who know to be cautious do not have the technical expertise and experience to independently decide whether a website is legitimate. R3a explained that she puts her information into websites when necessary, even knowing risks: *"Everything has risks – social worker, case managers – whoever you share your information with, you have no idea what they will do with that information. But if you do not provide your information, you cannot get what you are trying to get from them. It's a gambling situation. In order to gain something, you have to give up."*

2.5.3.4 Physical Documents Security

Because refugees frequently interact with various bureaucratic processes (e.g., with government agencies or potential employers) requiring identifying documents, they frequently carry these documents on their person. In some cases—and sometimes on the advice of case managers or teachers who encouraged refugees not to carry the original copies—refugees instead keep social security numbers and other PII stored on their phones, as well as photos of documents like passports and social security cards.

Whether carrying physical documents or photos of documents on (potentially unlocked) phones, the need to carry this information creates a risk for identity theft when this information is compromised. Further, the practice of storing these documents on the phones makes the protection of these phones—and their digital contents—important. Indeed, participants told anecdotes about lost phones (T2, CM2, CM3, R1a) and CM3 expressed concern about the resulting potential risk of identity theft (though none of the scam anecdotes we heard were due to lost phones or documents): *"She's like, 'When I go to these appointments, whether it's electric help, whether it's the housing help, they need the information, and I can't grab all the papers all the time, so I have on my phone.' And I said, 'Oh, **you have a bigger problem on your hand than just losing your phone.**' And it was unlocked, no code. I said, 'No.' I told her …'hopefully you don't get your identity stolen that way but social security, date of birth, and name, and addresses, **you gave it to them on a golden plate**"* [emphasis added].

2.5.3.5 Safety of Communications

Despite fleeing very real threats of state-sponsored violence, many refugees are no longer worried about violence or surveillance from their home governments once they resettle in the US because they feel sufficiently protected by the US government (T1, T2, T3, T4, CM1, CM2, CM3). In general, refugees also trust the US government since it brought them to the US, and say that they are not concerned about any potential surveillance from the US government (T1, T3, T4, CM1, CM2, CM3). "*They feel safe saying whatever they want to say because they come to this country, they know they have that freedom of speech and stuff. They're okay to say whatever they want to say ... Once [they]'re here, they feel like, 'Okay, I can voice myself now'*" (CM3).

For example, T3 told a story about a refugee who was in great danger in his country for filming human rights violations on his phone, but felt very safe in the US. In answer to a question about whether they or any of their clients would talk about politics outside Eritrea, since talking about politics inside Eritrea is dangerous, CM1 said: "*Outside, yeah. As you like, yes.*"

However, these concerns remain for some refugees, though case managers and teachers said that these refugees are exceptions to the rule. CM1 did indicate that some refugees censor themselves in the US as they did in their home country, out of fear of informants or other surveillance from their home country. The Syrian refugees we spoke with indicated that they would not talk about politics for fear of something bad happening to their friends and family who are not in the US: "*Here, we don't feel, you know, we aren't afraid of anything, we feel very comfortable here, but we are worried about our relatives in different countries, in Syria, to say something that might affect them*" (R1d).

Although few participants directly said so, some indicated that there was concern about the US government as well. For example, while deciding whether to consent to audio recording, one focus group participant asked whether the interview data would make its way back to the CIA. (We note that this participant did consent, and we received permission from our IRB to include this observation.) And although teachers and case managers said refugees were not worried about surveillance from the US, they told anecdotes in which refugees were uncomfortable with the information that they had to give out. CM4 said that Muslim refugees in particular might censor their speech or actions due to recent US politics, but also indicated that was not the majority.

Finally, some participants said that refugees preferred to conduct business in person. Related to refugees' attention to physical security, we found that they use non-digital and in-person information exchanges as a strategy for protecting information. R3a, for example, conducts business in person if at all possible after being scammed twice because she does not know how to truly verify identity over the phone or online: *"In person, yeah. If it's an office, I try to visit way ahead of time. If it's making a payment, I like to visit the actual location I need to submit my payments to instead of doing it online or over the phone. Because even over the phone you have no idea what they're going to do with that. Scary thing"* (R3a).

CM1 said that in general, when asked for information that could be given over multiple media, clients "*feel comfortable to give the paper rather than to send the picture*" but because they are extremely busy, "*they send the picture because of the time limit*" (CM1). The decision to share information only in person may have perceived or actual security benefits, but it can also create barriers to refugees' other goals, including establishing a life in the US (CM4).

2.5.4 Computer Security Advice Given to Refugees

Finally, we consider computer security and privacy advice given to refugees, either directly by case managers or teachers, or by others with whom refugees interact (e.g., friends or family). Similar to prior work on security advice more generally, understanding this advice helps shed partial light on the sources of refugees' concerns and practices [241, 244]. Because most or all of the people from whom refugees receive advice are not themselves technology or security experts, this advice reflects the (potentially incomplete or inaccurate) threat models or mitigation strategies of these people. Thus, interventions to improve security and privacy for refugees must consider this broader ecosystem of technology users.

General Constraints on Security Advice All teachers give some security advice (physical or computer) to their students in class, but T1, T2, and T3 expressed a desire to include *more* security advice in their classes (though we note that these statements may have been influenced by the fact that they were speaking to us, security researchers). They, along with T4, CM4, and CM5, identified time and resources (i.e., access to computers for teaching) as a limitation. CM4 explained that both time and the clients' own prioritization of computer skills (including secure behavior and mental models) are both limitations: "*They're adults. It's very hard in one shot to convince them that this is very important for your life, in day to day life. Just only delivering that information doesn't make them change, it has to touch their heart, it has to touch their soul, they have to feel it. Just giving them one lecture about the use of computers... It has to go beyond that.*"

Some of the same case managers and teachers indicated that they have advice that they do *not* give, either because their clients are not technically ready for it (T1, T2, T3), or because they, the case managers, prefer to let their clients make their own decisions (CM3).

Now, we turn to the concrete advice that case managers and teachers do give their clients about protecting themselves.

Advice about Protecting Personal Information from Scams Recall from Section 2.5.2 that case managers and teachers identified scams and identity theft as potentially new risks for refugees, and said that they try to instill an awareness of these risks. T4 and T1 talk to their classes specifically about phone scams. T1 advises their clients to "*just hang up*" if "*you get a call from a number that you don't know and they're saying something and asking you questions*," and T4 tells them about "*information that you never tell anybody over the phone because nobody will ever ask you for it*," like "*your social security number.*"

Like T4, CM3 also emphasizes the importance of not giving out social security numbers, and CM1 and CM2 said that refugees hear about the importance of keeping their social security number private from other sources, such as other, more experienced refugees from the same community.

The cultural orientation that refugees receive before resettling in the US also includes information about potential scammers and the importance of keeping certain personal information private. The orientation "*let[s] you know that there could be scammers, you should keep your personal information safe and in a secure place, you shouldn't share your personal information with others*" (CM1).

Advice about Website Identity Beyond general advice about protecting personal information, case managers and teachers also attempt to teach their clients how to avoid scam websites in particular. T1 and T3 send emails to their classes with links, and try to get their students to actually read the emails before clicking on links. CM1 tells their clients to "*use the link that they trust*," such as on websites that they already know, or printed on a business card.

CM1 alluded to a whitelist of company websites and job application URLs which they can send to clients, but when a company or job is not on their list, they either verify it themselves, or recommend the following strategy for checking: "*I google it, the nearest address of that company. I told him, this place is 15 minutes drive from here. I give him the directions —I mean, I printed out the map. Then I told him you can drive to the address, you can go in, and you can ask them for their business card. Or you can ask them how to apply on the website. If you get it from them, it's trustful...*"

However, no participant explained *how* they learn a new URL is safe, or what advice they would or do give to their clients about trusting a new URL without verifying it in person or on paper—perhaps because they themselves are not aware of foolproof strategies to recommend. This is a difficult problem even for digital natives, who may be more accustomed to looking for browser-level signs like HTTPS indicators or searching through search engine results.

Advice about Account Security Though teachers generally support their clients' security and privacy by teaching them how to protect themselves from scams, they typically do not include (email) account security or password hygiene. Their main goals with computer education are for clients to log in to their email addresses in a browser, send emails, read emails, attach documents, and log out, but creating the accounts or picking good usernames and passwords is a one-time process so it is not a priority (T1).

When case managers and teachers do convey advice about keeping email accounts secure and private, they advise their clients to remember their passwords and not to share passwords with anyone else (T1, T2, T3, CM5). We note that this latter piece of advice may be directly counter to the case managers' and teachers' own practices of retaining access to clients' passwords—again highlighting the tension between security "best practices" and the day-to-day requirements of their work, as well as subtle differences between whom a user may reasonably need to trust with a password and from whom passwords should be protected.

Case managers and teachers also impart advice about password creation, often while helping create or reset a password. This implicit (or sometimes explicit) advice comes in the form of the password creation algorithms the case managers or teachers themselves employ: "*I try to help them create something that's easy to remember, so I'm like, 'your birthdate, your child's name, or your child's birthdate'*" (T1). These strategies focus more on creating memorable passwords rather than creating secure passwords, reflecting the teachers' and case managers' assessment of their threat model for their clients' email accounts: they often encounter cases where clients have forgotten their passwords and need help accessing their accounts, but told no anecdotes about accounts that had been compromised.

Two teachers also mentioned teaching their clients to log off of their emails when they are done on the computers, "*so that when someone else gets on the computer, they don't open up your email address*" (T1).

Summary of security advice Overall, in Section 2.5.4, we observe that case managers and teachers seem aware of common security best practices around account management and avoiding suspicious websites—however, their technical knowledge may be incomplete, they may struggle with fundamentally hard usable security challenges (such as identifying phishing websites), and they may trade off teaching and practicing hypothetically stronger security measures with the need to achieve other goals (e.g., helping their clients find jobs as quickly as possible).

2.6 Discussion

We now step back to highlight key lessons and develop recommendations for the computer security community and other technologists designing for refugees; since refugees have significant overlap with other underserved populations, these lessons and recommendations may apply more widely to populations other than refugees.

2.6.1 Lessons

Refugees have heterogeneous technical expertise and threat models, and intersect with other vulnerable populations In our interviews, we encountered and learned about refugees with highly variable technical skills and experiences. This heterogeneity leads to a diversity of threat models, security-related actions, and effectiveness of existing or proposed security solutions. Some refugee subgroups share concerns and threats with other vulnerable populations in the US—e.g., people with low incomes, low literacy, limited technical expertise, or limited English skills—while others may not. The observation that "one size does not fit all" echoes recent work within the computer security community studying the needs of particular user groups (e.g., [99, 189, 195, 198, 217]). For example, the importance of studying vulnerable populations like refugees is highlighted by anecdotes from our study about scams targeted particularly at people looking for low-income housing or minimum wage jobs; similarly, many of the account practices of refugees are unique to their situations and relationships with case managers. Computer security researchers may not be aware of these threats or challenges without specifically studying the vulnerable populations that they affect.

Computer security is not a primary concern Echoing a common lesson in usable security, we observe that security is generally not a primary concern for refugees. However, unlike other user populations, refugees are often trading off security-related decisions not with convenience or functionality, but with existential needs that include finding a job, making an income, and establishing a life in the US. Thus, any computer security solutions or advice that impact the efficiency with which refugees can achieve those primary goals will be ignored or circumvented.

Common security mechanisms require cultural knowledge Many refugees share in common the fact that their entry and integration into the United States involves a major cultural shift. In addition to language and other barriers, these cultural differences can create barriers to establishing their new lives. We find that these cultural barriers also directly affect computer security. We observe that many common end user computer security practices rely heavily on US-based cultural knowledge and norms, including: the fact that social security numbers must be kept private except under certain circumstances (e.g., when applying for a job); the existence of scams and identity theft as a common threat (and the language skills needed to identify likely scams); the information requested by account recovery security questions; and the use of one's birth date as an authentication token. It is critical to identify such cultural assumptions embedded in computer security technologies and account for them in technology designs.

Common security advice and assumptions may be inapplicable to refugees Among the heterogenous experiences and needs of refugees, we observed cases in which common security advice may be inapplicable to them, or even counterproductive. For example, we found that refugees commonly share email account access with their case managers, due to the importance of finding a job quickly in the face of limited cultural, linguistic, and technical skills. However, this practice contradicts common security advice which instructs people, without regard for their situation, never to share access to accounts or account credentials. (For example, Apple, Google, and Microsoft all officially advise not sharing account credentials, even with friends or family members.[4]) However, following this advice can be counterproductive—for example, leading to refugees who are locked out of their email accounts due to forgotten passwords—and directly conflicts with a refugee's primary goal of quickly finding a job and settling in the US.

[4] `https://support.apple.com/en-us/HT201303`,
`https://support.google.com/accounts/answer/46526?hl=en`,
`https://www.microsoft.com/en-us/safety/online-privacy/prevent.aspx`

Refugees' computer security practices are limited by their sources of advice We find that refugees' computer security threat models and practices are heavily influenced by their case managers and teachers, who act as key facilitators of their establishment of a life in the US. Other refugees, friends, and family also provide security-related advice. As a result, the security-related beliefs and practices of refugees are composed of a patchwork of advice and anecdotes shared by people who themselves are typically not technology or computer security experts, and are thus limited by the gaps in their threat models or technical knowledge (echoing findings about a digital divide in prior work on security advice more generally [241, 244]). For example, though case managers and teachers often discussed attempting to teach their clients to be cautious about which links to click on and which websites to trust, they often did not describe concrete strategies for how to make these trust judgments. It is not reasonable to expect that everyone working with refugees (or other vulnerable populations) be a computer security expert—instead, this observation further emphasizes the need for usable security more generally.

2.6.2 Recommendations

Informed by our findings, we make recommendations for concrete technical directions that can better serve the security and privacy needs of recently resettled refugees in the US.

Security for public computer users Since many refugees do not have computers at home, we found that they frequently use public computers for personal activities, including email and job applications, raising a number of potential security concerns. Ideally, administrators of public or semi-public computers should anticipate that some of their users may leave behind sensitive artifacts (and may rely on accessing them later), like resumes, or logged-in email accounts, and implement technical protections to protect the users' privacy between sessions. This solution relies on the individual administrators of these machines, however, and to our knowledge, research methods for secure, trustworthy kiosks have not been widely deployed [103]. By contrast, we found that refugees frequently *do* have smartphones. One potential opportunity for future work is to leverage these personal devices to help provide security for personal accounts and artifacts on public computers.

Security education and training Refugees typically learn computer skills and security from people who are not themselves computer security experts, and thus whose advice is subject to the gaps in their own knowledge and threat models. While it would be unreasonable to expect refugees or their case managers and teachers to become computer security experts, there may be targeted education and training interventions that could be effective. Future work should consider how to most effectively train and educate non-experts, such as case managers and teachers, who educate, in high volume, a less technically-adept population. For example, we suggest that security advice take into account the unique needs and tensions of technology use in this population, such as the reliance on case managers for handling job-related emails—i.e., rather than advising people never to share account access, directing people to more secure alternatives that may better balance their security and access needs (such as mail delegation in Gmail[5]).

Password and account management Our results reveal that refugees need to share their email accounts with their case managers, and case managers need to be able to efficiently access many different email accounts—causing them to engage in practices that may violate common security "best practices," such as reusing passwords, using weak passwords, or storing them in plaintext files. We observe that there already exist technologies that case managers and refugees *could* use to balance these efficiency and security goals, such as password managers and email account delegation. However, we also observe that these existing solutions may not serve this particular use case. Password managers, for instance, may be difficult to use on a public computer, and not every password manager allows sharing credentials. Some email providers, such as Gmail, allow email account delegation[5], but this feature seems designed more for use cases where the primary account owner has an assistant—

[5] `https://support.google.com/mail/answer/138350?hl=en`

it would not allow the case manager to actually act *as* the refugee when replying to emails, and would not give the case manager direct access to the password, which they sometimes need for account recovery purposes. Furthermore, we observe that other account security measures, such as two-factor authentication, may be entirely impractical for refugees' use cases, as they would prevent intended access by case managers. These observations raise several challenges for future directions: When existing password and account management solutions are appropriate, how can knowledge of these solutions be imparted to refugees and case managers? And when existing solutions are not appropriate, how should other, more appropriate mechanisms be designed?

Design to leverage refugees' trust in case managers and teachers We learned that many refugees trust and rely on their case managers and teachers, who pass on a lot of technical and cultural knowledge. An area for future research is how to effectively leverage that trust and use technology to help case managers and teachers pass on their knowledge asynchronously and effectively. One example of existing work along this line is Lantern [29], a smartphone application that helps newer refugees leverage the expertise of more experienced members of the community by scanning strategically placed NFC tags in places like resettlement agencies, bus stops, or grocery stores. Based on our findings, we observe other such opportunities—for example, a browser extension or smartphone application—that could allow refugees to consult remotely with their case managers about their impression of the trustworthiness of a particular website, or check a site against a whitelist precompiled by the case manager, a practice that we observed occurring manually in Section 2.5.3.

Security for digital documents Another area where technology may be helpful for refugees is in providing security for digital documents, such as photos of sensitive documents that we learned refugees may carry on their (potentially unlocked) smartphones. There do exist smartphone applications for storing encrypted or hidden photos (e.g., KeepSafe[6]), as

[6] https://play.google.com/store/apps/details?id=com.kii.safe

well as digital wallet applications (e.g., DigiLocker[7]). Future work should study these types of applications in detail to determine whether they have the security, functionality, and convenience properties needed for refugees' use cases—and if not, develop new applications or other approaches that do.

2.6.3 Limitations

Finally, we present several limitations of our study that should be considered when interpreting our results.

First, although qualitative methods can be insightful probes into vulnerable or hard-to-access populations, such as ours, they do not allow for statistically significant results. However, qualitative work on the security needs and concerns of various populations is valuable, e.g., [99, 189, 195], and the depth of the results forms recommendations and lessons for future researchers. Additionally, there is inherent bias in any interview study, particularly about security and privacy, from the fact that participants self-select to participate. For example, it is possible that highly privacy-conscious individuals may be less willing to speak with researchers about technology usage and concerns, and this might skew our results.

Further, as discussed in Section 2.4, our sample skews towards refugees who rely on assistance from case managers and teachers, and may thus have lower English, technology, or other skills than others. Furthermore, our case manager and teacher interviews reveal their third-person perspective on the refugees they work with, rather than those refugees' own views directly. We valued the case managers' and teachers' perspectives spanning experience with many refugees and grounded in a deeper understanding of US culture. We also found that our refugee focus groups corroborated information we learned from the case managers and teachers. Because of our focus on resettled refugees who rely on case managers and teachers for assistance, many questions still remain about how resettled refugees' use of technology evolves, and what similarities they have to other groups, such as groups with

[7] https://digilocker.gov.in

low-income.

Finally, while we attempted to establish good rapport with all subjects—teachers, case managers, and refugees—it is possible that participants did not fully trust us. Although our interviews and focus groups surface numerous findings (Section 2.5), these results should be interpreted with the knowledge that our participants might have omitted more sensitive information.

2.7 Related Work

Finally, we present related work on refugees and technology in particular, and on computer security and privacy for different populations more generally.

Refugees and Technology Prior work studied refugees' use of technology in various stages of the refugee process; Talhouk et al. [292] broadly consider the role of the Human-Computer Interaction community in responding to the refugee crisis. Prior work does not consider computer security and privacy in particular, but provides broader context and in some cases surfaces security or privacy related findings. For example, Gillespie et al. [114] thoroughly overview refugee technology usage in and en route to Europe, including surveillance and physical risks as well as the use of social media to spread trusted information; Flemming [92] and Peterson and Fisher [231] study technology use among resettled refugees, particularly for communication with family and friends. Other work has studied technology usage within refugee camps, such as works that surveyed smartphone usage of Syrian refugees in a refugee camp [293, 326], works that studied a computer club in a Palestinian refugee camp [9, 10, 329], and work that broadly examined barriers to technology usage [179]. Other groups [67, 81] have examined the role of technology specifically for education in refugee camps.

Yafi and Said [327] consider WhatsApp usage by resettled refugees, and Almohamad and Vyas [19] more broadly examine the challenges faced by refugees and asylum seekers integrating themselves into host communities and present possible technical design interventions.

There also exist efforts to develop technology specifically to help refugees navigate their new communities, including Lantern [29], a smartphone app that connects new refugees with experienced refugees via NFC tags placed physically around the community; Rivrtran [40], a human-in-the-loop translation platform for recently resettled refugees; and RefUnite [5], a social network.

Computer Security and Privacy for Different Populations Our research echoes other recent work in computer security and privacy that has observed the importance of understanding the nuanced needs and constraints of different user populations, in order to best serve the security and privacy needs of those populations. For example, recent work has considered potentially particularly vulnerable user groups, including low-income people in the US [189], domestic abuse victims [99, 195], older adults [217], journalists [198], and activists [36, 130, 193]. Sawaya et al. [260] conducted a large-scale cross-cultural survey of security habits of people from seven countries, and find that security habits and knowledge vary across cultures. Similarly, Redmiles et al. [242] and Wash et al. [318] found difference in security beliefs and behaviors among different demographic groups within the US. Like many of these prior works, our work suggests that the population we study—recently resettled refugees in the US—have distinct computer security and privacy needs and constraints that must be understood before technologies can best be designed for this population.

2.8 Conclusion

Refugees are a potentially vulnerable population, relying increasingly on technology while attempting to establish lives in their new homes. We studied East African and Middle Eastern refugees recently resettled to the US to understand their interactions with and reliance on technology, the barriers they face in implementing strong computer security and privacy practices, as well as their existing security and privacy practices and the guidance they receive from their case managers, teachers, and others. We conducted in-depth semi-structured interviews with case managers and teachers who work with these refugees, as well as focus groups with refugees themselves. We find that refugees are highly dependent on technology and on their case managers and teachers to help them navigate that technology, and we identify numerous cultural, language, and knowledge barriers that impede or are otherwise in tension with commonly recommended computer security best practices. We draw lessons and recommendations for the computer security community, laying a foundation for technologies that can help overcome these barriers and better meet the computer security and privacy needs for refugees and other potentially vulnerable populations with similar barriers and needs.

Stepping back to the broader themes about change and vulnerability throughout this dissertation, I find that refugees experience an onslaught of new information, entities, and technologies, and they—understandably—are not always able to reason about it due to the volume of newness, which leads to incomplete threat models, which crates vulnerability (theme 1). I also find that many refugees are forced to deprioritize computer security and privacy in order to submit job applications, for example (theme 2), and that there are numerous design misalignments that increase the amount of work refugees in the US must do to maintain computer security and privacy, which exacerbate existing systemic inequities. Therefore, it is our responsibility as designers and technologists to realize that change makes refugees (and others) vulnerable in this way and to design better systems that actively support diverse users undergoing change.

Acknowledgments

We thank Richard Anderson, Zakariya Dehlawi, Nicola Dell, Kurtis Heimerl, Karl Koscher, Kiron Lebeck, Katharina Reinecke, Alex Takakuwa, and Reem Talhouk for early discussions and efforts on this topic; Eric Zeng for his insightful feedback on our paper; and Brian Rogers and Alison Simko for their copyediting. We thank Jialin Li, Danyang Zhuo, and Haichen Shen for helping us practice running a focus group. We thank Michelle Mazurek for shepherding this paper through the revision process. Finally, a massive thank you to our anonymous participants for giving us their time and invaluable insights.

This work was supported by the NSF Graduate Research Fellowship, NSF Award CNS-1463968, the Short-Dooley Professorship, the Marilyn Fries Endowed Regental Fellowship, and the Bill and Melinda Gates Foundation.

Chapter 3

DEFENSIVE TECHNOLOGY USE BY POLITICAL ACTIVISTS DURING THE 2018-2019 SUDANESE REVOLUTION

This chapter presents my work on how activists used technology during the 2018-2019 Sudanese revolution. Political revolution means a significant change in daily routine, can introduce widespread economic insecurity (as in the Sudanese revolution), and is a time of varied and increased threats and risks, especially for activists driving the revolution. This chapter explores how this change led to vulnerability, first exploring the three broad themes about change and vulnerability, and then presenting the research itself.

Change: political revolution. Political protest and revolution are a driving force of political change, and can be a tool to fight human rights abuse and dictatorships. In contrast to the individual and family-level changes that refugees undergo when moving to a new country, political revolution is a change on a regional or country scale. Revolution—or times of great protest or upheaval that advocate for major changes in policy—may bring **economic insecurity** to an entire city, region, or country, which can cause food shortages, unemployment, and general insecurity about the future. Protests and other forms of physically present activism may also be **physically dangerous** for those involved, and, recently, both personal technology (e.g., social media) [304] and **mass censorship and internet blackouts** [110, 185, 192, 209, 210] have played significant roles in political protest. Specifically in Sudan's 2018-2019 revolution, which began in response to the rapidly increasing price of bread [6], protesters were massacred during a peaceful sit-in, and then faced a 5-week-long internet blackout (Section 3.2 describes the revolution in more depth). Sudan's political situation has continued since the installation of the civilian-military government in July 2019, with further protests and regime changes, though this chapter focuses on the period from 2018-2019.

Theme (1): new threats, new or increased risks, changing actors. In contrast to refugees, who find themselves in a new location, revolutionaries face many of the same actors as before the revolution, but they face **increased risk** for violations of security and privacy, and may adopt **new technologies or new models of technology use** in response. During the Sudanese revolution, activists faced threats of **physical violence** from government officials, **surveillance**, and **internet blackout**. In response, they developed new strategies for using technology individually and as a group; some of the strength of their strategies, I believe, was the sheer variety of low-tech technical practices to evade non-automated or non-targeted surveillance, increasing the attack surface but dramatically lowering the benefit for the adversary to respond to any single strategy.

Their **adversaries also may change** throughout the revolution; in the Sudanese revolution, the original target, the dictator, was ousted in a military coup and the military became the new adversary until the activists reached an agreement with the military and installed a joint military-civilian government.

These changes in risk, threat, and adversary may happen suddenly, and due to the nature and capabilities of a government or state adversary, activists may have an incomplete or inaccurate threat model and thus be unable to appropriately meet their goals for their own security and privacy.

Theme (2): changing prioritization of digital security. As agents of change, revolutionaries push for political and social change and may prioritize these high level or long-term goals over their personal digital security and physical safety. In our study, participants expressed that they were, at times, scared for their physical safety and unsure whether their digital security measures were sufficient, but felt compelled to continue their activism despite these fears. Thus, even though activists may want to protect their digital security and privacy—and they recognize the connection between digital security and their own physical safety—**they may prioritize their goal of political change, and then fit digital security practices around that goal**, limited by the design of the technology itself, the resources available to them (which their adversary has varying degrees of control over), and group adoption of secure communication apps. This is, of course, a vast generalization, and not all activists will make this choice, but some do, as told by our participants.

Theme (3): political and societal context drives adoption of technology. Finally, this chapter is about how **political context drives technology adoption** both directly and indirectly: first, international and national policies can restrict what technologies are available (i.e., sanctions, censorship), and national laws about telecommunications and privacy can dictate the adversary's power, which may in turn drive users to adopt one technology over another (e.g., VPN adoption as a defense for censorship). Second, **the design of many popular technologies favors the privacy of those in the US and Europe**, who are protected by US privacy laws and/or GDPR. For example, Apple and Android phones have features to quickly and surreptitiously turn off biometric authentication; this benefits users in the US because it is far more difficult for law enforcement to compel them to give up an alphanumeric passcode or password than to authenticate through a fingerprint or facial identification. This feature does not protect users in Sudan, where privacy is defined differently. We found pervasive misalignments like this between technology design and Sudanese activists' needs. The activists, in many cases, found workarounds and developed defensive strategies that worked for their particular situation, but this shows, again, a theme that this population had to work harder to maintain security and privacy because the tools did not fit their context.

Co-authors and original publication. The remaining pieces of this chapter were published at the IEEE 2021 Symposium on Security and Privacy [66], and are closely related to an article in the IEEE Security and Privacy Magazine that appeared in 2022. In this chapter, I used “we” to represent the work and writing done by my coauthors, including co-*lead*-author, Alaa Daffalla, without whom this work would not exist and who had the original idea for this paper. The other authors are Tadayoshi Kohno and Alexandru G. Bardas.

3.1 Introduction

Though political activism has been a driving factor in geopolitical changes for centuries, the ubiquity of smartphones and social media has changed both the tools that activists use, and the extent of the legal and infrastructural power that states have over activists [304]. Activists fighting oppressive regimes increasingly incorporate technology in their daily activities, using it to share knowledge and organize. At the same time, their adversary may aim to infiltrate their groups, arrest them, or otherwise forcibly deter them. Political revolution, a dramatic culmination of activism efforts, puts technology used by activists under extreme stress because it may not be designed for those directly colliding with a state actor. Therefore, it is important to consider that while technology could support them, it could also make their tasks challenging or expose them to risk.

While significant progress has been made toward computer security and privacy for the general population, more work is necessary to address the needs of specific user groups. Indeed, there have been numerous efforts focused on specific populations (see Section 3.3 for an overview). However, political activists under an oppressive regime have not yet been extensively studied by the computer security community.

We suggest that it is fundamentally important for the computer security and privacy research community to (1) understand the computer security and privacy needs, practices, risks, and challenges facing activists under an oppressive regime and, specifically (in this work), during a national revolution. In doing so, it becomes possible to (2) empower future technology designers, policy makers, and researchers to consider if or how technology might best support the needs of activists under oppressive regimes or during a revolution. This understanding must provide technologists with a way to (3) reason about what issues might arise in the future, for whatever technology they are creating and for whatever world might later exist. Namely, technologists could benefit from guidance for reasoning about technology use during extreme political strife. In this work we provide a foundation for addressing all three of these gaps.

One recent revolution is the 2018-2019 Sudanese revolution, which resulted in the ousting of Sudan's president of nearly 30 years, Omar Elbashir. Our work focuses on the needs, practices, risks, and challenges of activists during this revolution, with larger inferences to future movements and technologies. Our insights stem from in-depth interviews with 13 Sudanese activists. The study received IRB approval from our institutions, and we took extra precautions given the sensitivity of this topic, as detailed in Section 3.4.

Stepping back, before presenting our research questions and findings, we first observe that activists have multiple goals during a revolution, for some of which they rely on technology.

- Activists must organize, attend, and publicize protests and other activities in order to push forward political change. Simultaneously, they must also keep up with international and local news.

- Because activist groups are always changing, with members both leaving (due to arrest) and joining (some of whom may be adversarial), activists must build trust with each other.

While activists do the above in order to achieve their political goals, they must also contend with their adversaries in different contexts. The governmental bodies against which they are rebelling push back using various tactics (including flagrant human rights abuses in some parts of the world [144]):

- The adversary may control or have influence over infrastructure upon which the activists rely.

- The threats may be technological, e.g., fake Twitter accounts spreading misinformation, or a complete internet blackout.

- The threats may be physical, e.g., arrest, violence, tear gas.

Some political activists may not have planned to become activists until the government started to exert some control over them or their technologies. Many activists are not technology experts and hence information within the community of activists informs their technology use.

With this backdrop, we formulated the following research questions. Our interviews were semi-structured, thus, individual discussions with participants also explored other topics.

1. What was the threat landscape during the revolution?

2. What were the activists' security practices? In what ways did technology and design support them or hinder them? To what extent did they feel their security goals were met?

3. How did activists adopt new technologies, behaviors, or mental models? Who taught them?

Through these questions, we learn, for example, that:

- **Politics and society are driving factors of security and privacy behavior and app adoption**. For example, the Sudanese diaspora played a significant role in passing knowledge to activists on the ground, and formed a robust ad hoc content moderation team on Twitter. Additionally, international sanctions on Sudan influenced app availability and pushed users to use a foreign phone number as a second factor for social media accounts.

- **A social media blockade can trigger a series of anti-censorship approaches at scale, while a complete internet blackout can cripple activists' use of technology**. Sudanese activists were unfazed by the censorship of social media; they constantly adapted by using VPNs or different apps (e.g., Telegram's adoption). In contrast, the 5-week internet blackout drove activists to analog techniques, including the use of a coded language over (surveillable) SMS and telephone calls. Group adoption of mesh networking apps such as FireChat [305] proved highly unsuccessful.

- **Activists' defensive strategies—against threats of surveillance, arrest, and physical device seizure—were low tech, yet largely sufficient.** This was in part due to the variety of defenses, requiring more work for the adversary. For example, activists meticulously deleted messages and logged out of social media accounts before going to a protest, or hid apps in other ways such as through iOS's ScreenTime [24] or Android's TwinApps [27] feature. However, many of these defenses cost activists preparation time and data loss, revealing that mainstream apps do not support activists' needs, even though activists can find workarounds.

- **Key principles for contestational** [135] **and defensive design could be better supported by current technical and UI design, but also may be in tension with each other.** We surface key design elements that our results suggest would aid those facing an oppressive government, e.g., support for mesh networking in mainstream chat apps, alternate authentication methods, or data sanitization or deletion on trigger. However, we also find that it is difficult to generalize these recommendations because they may be in tension with other recommendations—e.g., some groups may prefer to use mainstream apps, while others may prefer apps with a smaller user base. At a high level, our findings suggest that it is difficult to generalize specific design recommendations that fit *all* user groups, and that users should have multiple options, e.g., design *principles* should be implemented in ways that are adoptable (or not) by the user.

3.2 Background on Sudan

Sudan is a country in North Eastern Africa with an estimated population of 45 million as of July 2020 [306]. Sudan has had a number of governments following independence from British rule in 1956. In 1989, Omar Elbashir led a military coup and seized control of the country. As Elbashir's government gained power, Sudan established itself as a regional ally

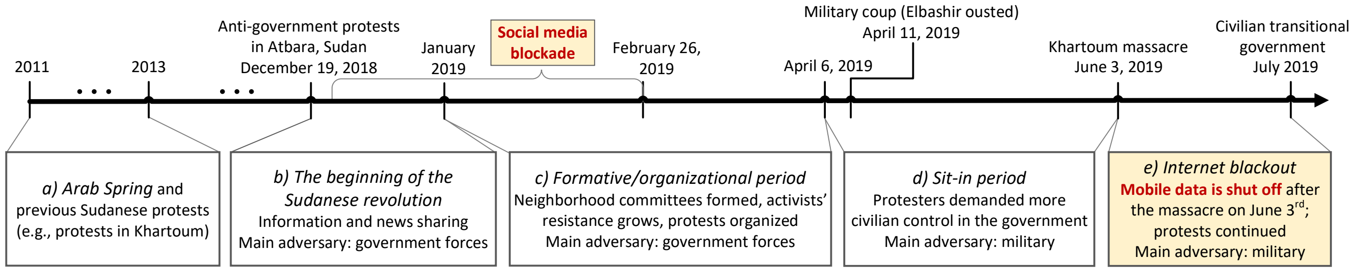

2011
2013
Anti-government protests in Atbara, Sudan December 19, 2018
January 2019
Social media blockade
February 26, 2019
April 6, 2019
Military coup (Elbashir ousted) April 11, 2019
Khartoum massacre June 3, 2019
Civilian transitional government July 2019
a) Arab Spring and previous Sudanese protests (e.g., protests in Khartoum)
b) The beginning of the Sudanese revolution
Information and news sharing
Main adversary: government forces
c) Formative/organizational period
Neighborhood committees formed, activists' resistance grows, protests organized
Main adversary: government forces
d) Sit-in period
Protesters demanded more civilian control in the government
Main adversary: military
e) Internet blackout
Mobile data is shut off after the massacre on June 3rd; protests continued
Main adversary: military

Figure 3.1: Timeline of the major events during and leading up to the Sudanese 2018 - 2019 revolution.

for Islamic fundamentalist groups while building a reputation for human rights abuses [144] and censorship of print and electronic media [145]. In 1993, Sudan was designated a state sponsor of terrorism by the United States of America (US) [307].

In the past decade, telecommunications operators in Sudan have built well-equipped infrastructure and expanded cellular and LTE services by connecting more than 10 million users to the internet as of 2016 [306]. Android phones are the most popular smartphones in Sudan, followed by iOS devices [205], in part due to US sanctions impeding access to services such as downloading and updating apps from the Apple store and accessing iCloud which requires a VPN connection [163]. Access to the Google Play Store was initially curtailed, but in 2015, as the US eased its sanctions, some Google Play services became available to Sudanese users [234]. However, access to paid apps/features remains restricted [118].

In 2018, due to the dire economic situation in the country, a wave of protests erupted and led to the 2018 - 2019 revolution [248]. Figure 3.1 captures the main phases of the Sudanese revolution, starting in December of 2018 and leading up to the formation of the civilian transitional coalition. Throughout the different phases of the Sudanese revolution, protesters were targeted by a number of state actors, including the police, the National Intelligence and Security Services (NISS or "the security services"), the military, and a special division of armed forces, the Rapid Support Forces (RSF). A more detailed glossary of state and non-state entities is available in Appendix A.3. As shown in Figure 3.1, the major events leading up to and during the Sudanese revolution are:

Arab Spring protests Sudan caught up on the early wave of the Arab Spring[1] when protests erupted in 2013 following unrest in neighboring countries. These protests were suppressed by the Sudanese government. In these uprisings, social media played an important role in promoting collective activism, with Facebook and Twitter among the most popular social media platforms for participating in protests and facilitating protest logistics [303, 304].

The beginning of the Sudanese revolution Initial protests erupted in the city of Atbara on December 19, 2018. Within days, demonstrations were held in most cities across Sudan. An umbrella organization of professionals' groups and unions, the Sudanese Professionals Association, emerged as an organizer and a leader for the protesters and became a reliable source of news [11]. As the protests gained momentum, on December 21 the government curtailed access to popular social media platforms including Facebook, Twitter, Instagram, and WhatsApp. According to NetBlocks [208], blocking measures were decentralized and carried out at the discretion of the telecommunication operators.

Formative/organizational period Protests continued throughout this period. The movement evolved to become more organized and structured with neighborhood resistance committees being formed. Neighborhood committees were groups of activists who came together to lead the movement at a local level, acting as a robust information network covering the country while serving as independent and decentralized resistance hubs that worked under anonymous leadership [12]. Due to the growing support for the protests among the population and the pressure from the international community, the social media blockade ended towards the end of February 2019 [208]. On April 11, Sudan's president Elbashir was overthrown after tens of thousands of protesters encircled the military headquarters in the capital,

[1] A wave of democratizing protests/revolutions throughout Middle Eastern and North African countries, including Egypt, Tunisia, Libya, and Yemen.

Khartoum. Following that, a Transitional Military Council (which included the RSF) was formed to pave the way for a civilian rule.

Sit-in period The protesters feared that if they left the massive protest scene in front of the military headquarters, their revolution would come to an end and their demands for a civilian rule would not be met [228]. So they stayed, creating a mini-city or sit-in area in a matter of days. The area had no cell towers; hence, mobile communications and internet access were limited. Most people relied on in-person communication. While the Transitional Military Council was still in power during this period, there were no violent attacks on the protesters and, according to our participants most people felt safe in the sit-in area.

The Khartoum massacre and the ensuing internet blackout On June 3, armed forces brutally attacked those in the sit-in area in an attempt to disperse the protests, leading to the deaths of 120 people and injuries to more than 700 [22]. At the same time, the regime shut off the internet throughout the country. However, after a few days limited internet access was available through landline service providers since many vital institutions, such as banks, required internet service to operate. In contrast, internet (data) from mobile carriers was completely shut off, leaving most without data connection due to the low rate of home and public Wi-Fi networks [306]. The blackout continued for more than a month until an agreement between the military and a coalition of political parties was reached to form a civilian transitional government.

3.3 Related Work

Our work is informed by prior work on activism, security and privacy for specific user populations, and adoption of security behaviors. We summarize these efforts below:

Surveillance and censorship Censorship-oriented research has focused on China (e.g., [52, 62]) and other parts of the world such as Saudi Arabia, Iran, and Bahrain [113, 313], or

Thailand [106]. Groups have also focused on the commercial tools used by nation states for surveillance and censorship, e.g., Blue Coat [37]. While the studied techniques include keywords, IP addresses, and hostname filtering, Sudan additionally experienced a different type of censorship during the revolution: an internet blackout. Internet blackouts have occurred in the past decade during revolutionary movements or uprisings [69]. For example, internet shutdowns happened in Egypt [250], Libya [290], and Syria [93] during the protests that erupted in 2011 and 2012, and in 2019 and 2020, there have been blackouts after protests in Belarus, Ethiopia, India, Iran, Venezuela, and others [110, 140, 192, 209, 210].

Activists and technology Activism involves advocating for social, political, or environmental change, tackling issues of injustice or uncovering corruption. Others in HCI have studied activism, e.g., health activism [59, 119, 225] or feminist HCI [79, 89]. Along the lines of political activism, Tadic et al. [291] 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. examined how professional activists decide when to use encrypted email [105]. Other groups have studied technology during political events, e.g., protesters during the Arab Spring [138, 184, 284], and by political refugees or other persecuted populations [73, 78, 121, 224, 232, 271]. Finally, in a series of studies on how to design 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 [135, 136, 137].

Security & privacy for vulnerable populations or in non-WEIRD contexts Prior works have found that security and privacy practices differ between cultures and countries [32, 50, 260]. Others have focused on specific non-WEIRD (Western, Educated, Industrialized, Rich, Democratic) populations, such as work focused on the privacy and security concerns of Saudi Arabians [235] or South Africans [246]. For example, the latter found that privacy practices of users living in South Africa were heavily influenced by their sense of physical safety which is different from a Western country [246]. Additionally, studies on vulnerable populations also present some overlap with non-WEIRD groups. Among these populations are studies of journalists, refugees, survivors of human trafficking, and undocumented immigrants, which have broadly found that vulnerable populations have heterogeneous needs that may not be met by standard security assumptions made by developers [47, 121, 197, 271]. We expand on this work by revealing key factors that could guide future researchers and technologists when designing for specific populations. We encourage future researchers to systematically compare and contrast the technical recommendations, threat modeling, and user practices in vulnerable populations as a step towards understanding how to generalize findings about specific populations.

Adoption theories A number of theories explain how behaviors spread within a given population. For example, in the Diffusion of Innovation theory, Rogers talks about the importance of communication channels in influencing the decision to adopt or reject a new idea or behavior [255]. Rice and Pearce expand on the Diffusion of Innovation theory to come up with the Digital Divide framework that examines the socioeconomic inequalities in developing societies through the lens of the adoption of mobile phones [249]. We build upon these works to provide an analysis of technology adoption, but as this is qualitative work with an exploratory objective, we do not contribute to the theory literature.

Adoption of security behaviors Researchers have examined how specific factors influence the adoption of security and privacy behaviors. Das et al. concluded that social triggers were the most common triggers influencing security and privacy behavioral change [70, 71]. Wash and Rader identified the importance of narratives and their consequences on how computer users conceptualize security threats [233, 317]. Abu-Salma et al. found that social influences or recommendations for adoption that come from the participants' immediate social network were among the main criteria influencing participants to adopt a communication tool [14]. Our findings also reveal the importance of narratives in user adoption of behaviors and technologies (as detailed in Section 3.7).

3.4 Methodology

We uncover key political, social, and technical factors that influenced activists' use and adoption of technology during the Sudanese revolution through semi-structured interviews. Our team was well positioned to conduct this research by combining security and HCI expertise. One of the lead researchers and interviewers is Sudanese and was in Sudan during the revolution, providing us with guidance on how to navigate the Sudanese cultural and political landscape, and serving as a layer of validation.

Recruitment process To recruit participants, we reached out to known Sudanese activists; we omit specific strategies for finding the activists, for safety, but note that future researchers seeking to study activists may need to invest significant resources to find and build trust with activists.

In each initial message, we explained that we were academic security researchers studying the technology practices of activists during the Sudanese revolution. At the end of each interview, we asked the participant if they would be willing to either pass our contact information to any other activists, or share other activists' contact information directly with us after receiving their consent. However, we deferred to the participants' comfort level, being cautious to respect their boundaries with sharing information of other activists soon after a revolution in which the very information we were requesting was highly protected and could have previously resulted in physical harm to one or both parties. Ultimately, 4 participants were recruited through snowballing.

Semi-structured interviews and data analysis We do not aim to quantify any one mental model or technical defensive strategy in the Sudanese activists community. Thus, we conducted semi-structured interviews, a qualitative tool commonly used for inquiry into vulnerable or understudied populations, e.g. [47, 197, 271]. We conducted 13 interviews with 14 activists of various experience levels, providing data with both depth and breadth, until reaching *thematic saturation*. We dropped one participant from our study after the interview because they did not identify as an activist, so we report on data from 13 participants (12 interviews). One interview had two participants (P7 and P8) because the participant we were planning to interview asked if their friend (who was also an activist) could join. In the interest of participant comfort, we accepted, but acknowledge that this interview had some of the drawbacks of focus groups, where a participant may choose not to share information that they do not want the other participants to know, or they may not share a story corroborating what the other participant has already shared.

We gave participants the choice of an interview in Arabic, but preferred English interviews because it meant two researchers could join instead of one. Ultimately, 5 interviews were conducted in Arabic by one researcher (who speaks Arabic natively) and the rest were conducted in English by two researchers (including the researcher who speaks Arabic). In the English interviews, participants were given the option to switch to Arabic at any point; some participants exercised this option for individual questions.

In our interviews, which lasted approximately one hour each, we asked participants first about news and information sharing during the revolution, a less sensitive topic. We then dove into more sensitive questions about general technology use by activists (e.g., for inter- and intra-group communication), threat models throughout the revolution, and the role of technology in protecting protesters on the ground. We also specifically asked about technology use and adoption during the internet blackout if it did not come up organically. A summary of our interview protocol is in Appendix A.1.

For analysis, we first transcribed the recordings. The researcher who is a native speaker of Arabic translated the interviews from Arabic to English. We then developed a qualitative codebook through an iterative process in which we created memos, open codes, and then coalesced the open codes into hierarchical axial codes. Two researchers then applied the codebook to each interview, continuing to iterate through two full rounds of coding. Using Cohen's Kappa, intercoder agreement was 98.7%. To fully capture the landscape of technology use, we coded 'Yes' for behavior that the participant knew *of*, regardless of whether they used any given strategy personally.

Participant safety and ethics Our study was approved by our institutions' Human Subjects Departments (IRB). Additionally, due to the sensitive nature of the topic, we took precautions to minimize the risk to participants. Most importantly, we let participants' own comfort level define their experience by giving them choices, including the technology we used to contact them and the amount of information they shared with us before and during the interview. All participants agreed to be recorded. Most participants preferred audio-only calls over video; in the interest of building trust, we kept our video on even if they did not. We also only collected enough information from participants to contact them on the day of the interview and did not pay participants, as our institutions required collection of name and address in order to dispense any payment, and international sanctions also prevented us from paying participants who were physically in Sudan.

Throughout the interview, we reminded participants that every question was optional, and that if they told us anecdotal stories, we did not want or need to know the names of the people involved. If participants seemed uncomfortable or reluctant, we changed topics or ended the interview, though we perceived this happened only once, which we attributed to the participant being tired because it was late in their timezone.

Looking beyond our specific procedures, a separate ethical question emerges about whether the publication of our results will ultimately help or harm the efforts of future activists. For example, will the findings in this report allow future governments to prepare for—and thus stifle—future activists? Our findings suggest that it is unreasonable to expect that all future activists will be technically sophisticated. However, it is reasonable to expect that government and state actors will have technical sophistication. Thus, we believe that while our findings can contribute to the creation of technologies to empower future activists, we do not believe that our findings go beyond what a sophisticated government could deduce. In short, we believe that publishing these results will be a net positive for activist communities.

Limitations Although our sample size is sufficient to conduct a qualitative study due to reaching thematic saturation, our results should not be interpreted quantitatively. Additionally, we were unable to recruit participants from cities or towns in Sudan other than the capital, Khartoum, so activists from other parts of Sudan may have had different threat models or defensive strategies. However, because the activism and political movement is led from Khartoum, we argue that our participants represent an important population to be studied.

Also, it is possible that many of the participants did not fully trust us, so may have not revealed their most sensitive information, but given the candor with which most of them spoke (or said they wished to skip a certain topic), we do not think they would have provided inaccurate information.

Participant overview For the safety of our participants, we did not collect demographic information, and we use they/them pronouns to mask participants' genders. Collectively, we report that of our 13 participants, 3 were female, meaning that men are overrepresented in our dataset, especially for a revolution in which women played a vital role [187], though prior work has observed gender differences in specific activist contexts too, e.g., hacktivism [296]. We believe the demographic imbalance is a consequence of our recruitment method, and while balance was a goal, our main goal was to simply recruit any activist who was willing to speak with us.

We also did not probe participants about their prior activism or their specific leadership or organizational role in the revolution. However, we do report information that participants spontaneously disclosed in the interviews: three participants said that they were part of neighborhood committees; two were part of the diaspora, and additionally, three were in Sudan for only some of the revolution. Two participants indicated they played a leadership role outside the neighborhood committees. We note that additional participants may fall into the preceding categories but may not have identified as such in the interview.

We present results from our qualitative interviews through the next three sections as technical, political and societal factors that drove the technical defensive strategies used by revolutionaries in Sudan. These factors emerged as natural classifications of topics from the interviews and form a lens through which to examine, anticipate, and explain the use of technology and defensive strategies in many contexts, including in other political movements, during internet blackouts, and against technically oppressive state actors.

3.5 Technical challenges: technical problems and app inadequacies drove adoption

In this section, we identify four fundamental technical challenges that drove activists to adopt a diverse set of low tech solutions. However, based on their stories, the *variety* of their defenses provided sufficient security by not giving their adversary one singular defense to focus on breaking. This section concludes with the actual security advice that participants received and which informed their technical practices.

3.5.1 Misinformation challenges mitigated through manual heuristics, crowdsourcing, and some platform affordances

Verification of information is a hard technical problem; politically motivated misinformation is rife throughout social media [285]. In Sudan, online misinformation was rampant during the revolution, though some participants considered it only a low-level threat (P8, P11). Misinformation originated from online accounts ("electronic chickens") paid by the Sudanese government [16, 288]. Misinformation ranged from fake news, to false reports about deaths at protests (P9), to false protest times and locations at which the police would be waiting to arrest activists (P5).

Some app features supported activists in building trust and disseminating verifiable information—such as livestreaming and the ability to report spam accounts—but activists largely relied on nontechnical methods to fact check. Additionally, some anti-misinformation policies on social media that are intended to reduce misinformation subvert activists' need to manage multiple online identities without pollution or context collapse, while heavily favoring an adversary that has control over the telecommunications infrastructure and companies.

Pre-trusted sources 8 participants said that the Sudanese Professionals Association (SPA) was one of the only trusted sources of news during the revolution, especially in its earlier days: "*All the people agreed on the SPA Facebook page as the official and only source of verified information*" (P2).

Other sources of news were verified or well known activists who built trust over time well before the revolution: "*On Twitter, most of the activists are well known.... It's a circle of well known people, circles intersect with each other. So there is a system in place to fact check the news*" (P12). During the internet blackout, activists reverted to trusted mass media: "*During that period, television was the primary source of information. So we were closely following two channels, Aljazeera and Sudan Bukra. We got confirmed reports from these channels*" (P2).

The search for first hand sources Activists built networks of contacts to enable them to 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 network between the sources and the destination. P9 constructed such a network in order to get to first-hand sources and verify news about deaths. P9 described their process to verify one such (alleged) death that happened in another city, in which they contacted a local friend whose family was from the other city, and that friend contacted their cousin, who found a doctor who worked at the hospital on the reported death date. They said: "*There was a chain of people who every one of them knows only one person. Even if they arrested, say, the doctor...they will find his phone and they will find 200 contacts. Are they going to arrest every single one of them? No. So there was no way to reach me, because I didn't contact* *the doctor.... There was no way to link all of them together unless they were very very very smart — and, believe me, the NISS wasn't that smart.*"

Fact checking through manual heuristics None of the participants mentioned platform affordances explicitly built to aid fact checking (e.g. Facebook's info button), instead searching through unknown online profiles to identify patterns of fake news or suspicious handles, echoing Geeng et al.'s findings about how users investigate misinformation [108]. P11 explained one of their heuristics: "*if someone's account is AhmadXYZ234567, then everyone knows that's a troll. But if someone's name is AhmadHussein08, and he's having normal conversations, but like misleading or misinforming, or spreading fake news, then that's more dangerous.*"

Additionally, P3 helped create and share infographics about how to fact check; however, no other participant mentioned seeing or using these infographics. Another fact checking strategy involved checking news across different platforms. P12 used Twitter to fact check Facebook given that Twitter does not allow tweets to be edited, unlike Facebook which does allow users to edit posts. P12 also believed that misinformation was both most common and easier to spread on Facebook and hence required additional efforts from the activists' side to fact check on Facebook.

Crowdsourced content moderation The Sudanese diaspora formed a content moderation team on social media, taking shifts and reporting and questioning suspicious online accounts (P11). P11 said that the content moderation community "*somehow... just became an organic expanded community, and the trolls would get shut down and reported right away.*" This ad hoc, organically crowdsourced, and effective (by P11's reporting) content moderation team may suggest that crowdsourcing and self-moderation can be effective within activist communities.

Producing verifiable information Activists were also dedicated to producing information that would be unalterable and therefore trusted. 5 participants mentioned livestreaming as a way to produce information that others consider trustworthy (P6, P7, P9, P11, P12), despite it being a physically dangerous activity: "*[Live broadcasting] is one of the most dangerous activities, especially when you are dealing with a regime like the former regime, who was shooting anyone who was using their phones to document a protest*" (P8).

P7 and P12 used verbal or written measures indicating the date and time of protests when livestreaming or taking photos in order to increase verifiability: "*Facebook became more reliable when people actually wrote a paper that has the date, place and time in addition to saying it verbal*" (P12). Activists' ad hoc measures to fingerprint their own reporting suggests that mainstream social media platforms should work towards enabling automated and human-verifiable fingerprinting.

3.5.2 Confidentiality over an adversarial network

Activists in Sudan were working under an adversarially controlled internet and telephone network. Except during the blackout, all used end to end encrypted (E2EE) chat apps such as WhatsApp or Telegram, which some perceived to be more secure because "*they have the self-terminated messages. So the conversation erases itself over 5 minutes, 10 minutes or something*" (P11). Furthermore, several had additional strategies in place to maintain privacy over these popular apps and they believed these strategies helped them stay more secure: P7 used a VPN to access WhatsApp, P13 used WhatsApp on an Android emulator instead of on their smartphone and obscured their network activity through intermediary servers, and P9 used the web version of Telegram.

Foreign Numbers as 2FA 9 participants mentioned adding a foreign phone number to their Twitter or WhatsApp account instead of their Sudanese phone number, with three strategies for doing so: first, some obtained foreign SIM cards, and used those SIM cards on roaming (P1). We observe that though this made participants feel safer, because they believed the Sudanese government could not intercept their texts with a foreign SIM, this may not have provided privacy guarantees against interception or after-the-fact-reading for an adversary with purview over the telecommunications companies.

Second, some created fake US numbers online through a "phone service in an app provider" (P14 gave this advice), thinking that this would provide privacy by not going through the Sudanese telephone network, but relying on the security of the app provider and depending on the internet availability.

Third, others "*ask[ed] their friends and family overseas to verify their Twitter accounts by using their numbers over there*" (P1). This strategy provided the security of having their 2FA not go through Sudan, but required waiting for a message from someone who might be many time zones away when using the second factor, e.g., after getting locked out due to VPN usage making the logins appear suspicious (P1).

Low tech defensive strategies With an entirely adversary-controlled network—including the possibility of apps backdoored upon download and fake cell towers at protest sites [116, 172]—activists did not find a wholly technical solution to ensure the confidentiality of their communications, and instead turned to a variety of solutions to supplement their preferred communication mode, relying on solutions that could not scale due to manual effort or hardware availability. Defensive strategies included using coded communication (8 participants) and making calls only over VoIP (not possible during the blackout, 3 participants). Others still used burner phones (9 participants) or burner SIM cards (7 participants) to distance their activist communications from their personal phones. P2 said that fake SIM cards were not difficult to come by, and that they did not require registration: "*there were a lot of fake SIM cards that people could purchase.... People can buy them without registering any sort of personal information*" (P2). We note that having either a burner SIM or a burner phone—but not both—may not provide the anonymity that participants thought they had.

Safety in numbers During the blackout, many started using SMS and telephone calls to communicate (11 participants), despite the fact that most participants believed the government had full access to SMS and telephone calls (12 participants). Some took no further action to obfuscate their communications because they felt the government could not effectively process all the SMS and call data it had access to. P5 said: "*the numbers were big – everyone in the whole country was talking about the same thing: protests, killings. So looking for specific keywords via voice recognition, it would not work. The whole country is talking about it. It's a revolution.*" 7 participants said that safety in numbers is contingent on whether an activist is a target of the government.

3.5.3 Availability of communication on an adversarially controlled network

Through this section, we explore how the government's ability to partially or wholly censor the internet drove adoption of different communication methods — for example, Telegram and VPNs, during the social media blockade, and SMS and telephone calls, during the mobile data blackout. However, we observe that such adversarial control of app usage could have been purposeful, leading people to a communication method that was compromised (e.g. how many suspected the government could access SMS records and track phone calls, or—our conjecture—an app with a backdoor or traffic routed through adversarially-controlled servers [116]).

Reliance on VPNs to circumvent the social media blockade In response to the government censorship of popular social media apps during the social media blockade in December 2018, some activists adopted various VPNs (7 participants). VPN usage allowed them to continue using the apps they were previously using, and added the additional security and privacy properties of encrypted and tunneled communications. Though P2 "*only used VPN during the... government enforced ...blockade on social media apps*," others continued using VPNs for their privacy properties (P5, P11, P12). P12 explained that "*even after the social media blockade...people were advising that to maintain your privacy it's better* *to continue with VPN uses especially if you were very active on social media*" — echoing Namara et al.'s findings [206] that users are driven by fear of surveillance when adopting VPNs.

However, P2, P6, P11 and P13 mentioned that VPNs would sometimes stop working, leading them to either search to find a new VPN or to stop using a VPN altogether. P13, a technical expert, attributed this to the Sudanese government blocking requests by IP ranges after a VPN became popular. P14, another technically experienced activist, began developing a VPN app that would help "*those who found difficulties with these international VPN apps.*"

Furthermore, when asked about the use of other more advanced anonymous network technologies like Tor, P13, a technically experienced activist, was against advice that would publicize the use of Tor because of a few (perceived) usability concerns: "*even if we use a Tor browser or gave advice for people to use it there are simple tricks or advice if people ignore it, for example while using a Tor browser don't minimize the screen because the moment you minimize the screen if someone is tracking you, you could be identified.*"

The shift to unblocked apps during the social media blockade In addition to VPNs, some activists adopted use of Telegram because it was not blocked during the social media blockade (P2, P6, P11, P13, P14). Others said that despite the blockade, WhatsApp and Twitter remained more popular (through the use of VPNs) (P5, P7, P12). We observe that the Sudanese government's power to influence app usage by blocking and unblocking apps could have funneled activists to specific apps that were advantageous to their adversary. Additionally, VPNs and other apps may be compromised or employ flawed implementations [146].

Group adoption of mesh networking apps during blackout faced difficulties The internet blackout was also a period of (attempted) adoption of new apps and communication methods because most of the apps that activists had been using relied on an internet connection, which was not available. However, many activists did not sufficiently fill their communication and confidentiality needs during this period. Some turned to SMS after attempting to adopt Firechat or Signal Offline Messaging, both mesh networking applications (6 participants). There were a number of reasons why participants failed to adopt mesh networking apps during the blackout, including the lack of group adoption and buggy applications or usability issues. Some struggled with operating the app itself and did not give specific reasons besides the fact that they couldn't make it work. P13 attempted to develop a mesh networking app after failing to operate Firechat: "*there was this app called Firechat but people couldn't make it work. We even tried it but it didn't work. It didn't even join those who were in close proximity to each other. So we tried developing an app.*" However, they failed to deploy the app before internet access was restored: "*We were in the testing phase when the blackout was lifted.*"

Moreover, 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. P1 said: "*[FireChat] didn't really work out because you had to have a large number of people who had Bluetooth on all the time, constantly, and they had to be next to each other, like actual next door neighbors.*" Furthermore, according to P14: "*We tried Signal at that time and tried to build a network but it wasn't effective. It wasn't effective because we wanted a communication tool with a larger reach.*"

More generally, another problem of mesh networking chat apps is the issue of download and setup without internet connection: "*There was a problem of, okay, it's an application, how am I going to download it while I have no access to the internet*" (P12). 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, recent research has revealed vulnerabilities in Bridgify, a mesh networking app popular outside Sudan [17].

Thus, we find that mainstream apps are developed with too-rigid threat models with respect to *availability* over an adversarially-controlled network, and apps specifically developed for use under an adversarially controlled network—i.e. mesh networking apps—struggled with adoption during the internet blackout. These complexities point towards mesh networking and connection robustness as a design principle to be incorporated into mainstream applications.

Other methods, including use of foreign SIMs and satellites Activists also found a number of alternative communication channels, though none were scalable. Some activists acquired foreign SIM cards which worked on roaming data and hence allowed them to resume normal use of mainstream chat apps, though we observe that the use of foreign SIM cards may not have given them the privacy they thought they had (P1, P9, P11, P12). P11 described: "*everyone was kind of scrambling trying to get SIM cards to be roaming from like USA, Qatar, Egypt, all of that.*"

Others relied on those in their communities who had home internet to relay messages. There were a few landline service providers operating at the time who provided internet access to government institutions and some home users: "*One of the providers had one of its services working which is like Sudani DSL*" (P11). P1, who had internet at home, explained: "*what I used to do is relay messages to people who are not in Sudan and keep them informed about what is going on every time I get a chance.*"

In addition, activists largely turned to SMS and phone calls to continue communicating with each other (11 participants). To recreate the group nature of WhatsApp and Telegram, some moved their WhatsApp contact lists to SMS (P1); others created phone trees, like P5: "*everyone who's somewhere and they witness something happening, they would write ... an SMS, send it out to all of their list, their trusted people. And you have to spread that at least to 10 people if you trust the source.*"

Four participants (whom we keep anonymous) also worked to smuggle in alternative infrastructure options, e.g., satellite internet equipment, in order to provide internet scalably and with less threat of government intervention, but expense was an issue, and "*getting it into the country was a whole thing, because it's not something that, you know, you could just* *ship and it looks like biscuits.*"

Finally, activists also used analog communication channels such as pamphlets and public graffiti (P2, P8, P11), which were relatively anonymous, but cannot replace phones.

3.5.4 Device security against a physically present adversary or upon threat of arrest

In anticipation of arrest and physical compromise of their phones, activists used a variety of low tech defensive methods to hide or remove data. P12 reasoned: "*it's better to burn what they have than to risk the data on their phones getting into the wrong hands and risking their security and that of others.*"

Manually hiding or deleting information Participants manually deleted or hid information like contacts, WhatsApp or SMS messages, group chats, images, and social media accounts with anti-government or activist posts (8 participants). Some formatted their phones entirely, relying on backups (P14). P1 planned to uninstall WhatsApp and Twitter and rely on cloud backup if they were arrested, since they had two SIM cards and the second SIM provided plausible deniability. They also archived messages regularly. P11 used iOS's ScreenTime—a feature intended to promote time management by hiding apps from the user—to hide social media apps at certain key times, for example, 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, though a complete lack of, for example, WhatsApp messages might be considered suspicious (P1). 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.

Decoy or alternative information Some activists also employed low tech strategies to increase plausible deniability if arrested: 9 participants added decoy social media accounts, alternative names for contacts on social media, or decoy messages on their WhatsApp accounts. P5 added a picture of Elbashir as their phone background, so as to appear pro-government if arrested: "*we had a joke, between me and my friends—we had our president's picture as wallpaper.*" As mentioned, P9 was released and deemed a non-activist after being arrested despite providing authorities their phone passcode: their release was due to their meticulous use of both manual information hiding and decoy information.

Going without technology Those who did not feel sufficiently protected by the available strategies chose to leave their phones at home and forgo any connection in favor of no liability (9 participants). According to P2: "*We spent a lot of time trying to delete information from our personal devices so I was one of those people who stopped carrying around their personal phones when going out in protests. Because we did a lot of different preparations. A lot of prearranged agreements were made regarding timing and location of meetings.... All of the agreements we made could lead to other people and put them in danger. So this is not only about me but about others who I might have communicated with during that day or the few days prior to the protest. So, as I didn't know about any technique that could hide information it was much safer to keep my mobile phone at home.*"

Reliance on group adoption of security measures As P2 said, security of the group was also part of the activists' decision to adopt certain security mechanisms: if one person in the group had poor security practices and was arrested, the whole group could be caught. Therefore, group adoption of security practices was critical, but activists could do little to ensure that their peers were truly following the same security strategies. For example, P9 used WhatsApp read receipts to signal to their contacts that they should delete the messages they had sent, but also admitted that there was no way to enforce this rule: "*you can't force someone to do something they don't want to do.*" P14, a WhatsApp group moderator put forth a set of conditions for those joining the group: "*We would send them a PDF document with all the measures they should take*" and "*Anyone who wasn't complying to this was excluded from the groups.*" The strong need for group adoption of security measures suggests that within group chats, apps could enforce self-terminating messages as a rule of joining a group, adhering to a broader design principle of enforced self-moderation also found in Section 3.5.1

Additional (burner) hardware Some relied on burner hardware (phone, SIM, or both) in order to ensure they did not have incriminating or identifying information if they were arrested (7 participants). We note that unless the activists used both a burner phone and a burner SIM, the metadata transmitted by their phone / SIM combination would link their identity. P13, a technical expert, explained their cautious approach: "*No one carried with them their smartphone. From when the protests started erupting we all went to the market and bought burner phones. We even bought new SIM cards for the burner phones. Our goal was to be in the safe side in case anything happened, nothing would be leaked.*"

Technology-supported strategies Less commonly, participants used apps or OS features specifically designed to conceal or delete information from their phones. P6 and P12 each used features from their Huawei phones to conceal information: Private Space, which allows users to conceal certain information behind a secret pin, and Twin Apps, which allows users to make a secret second copy of an app. For P6, these features provided sufficient protection, as they chose to not employ any other defensive strategies. In addition, P5 talked about an app that "*clears all of your data, and it sends out a message to pre-specified numbers that you got arrested.* Others relied on Telegram's self-deleting messages (P5, P11, P12, P13).

3.5.5 Security advice among the activist community

Now we turn to the content of the security advice that participants received. We find, broadly, that the common advice shared within the Sudanese activist community did not echo general-purpose advice given by the technical or academic security community (e.g. [42, 150]), though it does have similarities with activist-specific advice given to protesters in the United States in 2020 [311].

Advice: sanitize phone before a protest Most commonly, participants received advice about sanitizing their phones or social media accounts, particularly before going to a protest (P2, P3, P8, P12). P2 said: "*Once people became a little bit organized around April, people were shown how to deal with their mobile phones and how to delete things,*" including manually deleting messages, removing information from social media accounts, logging out of social media accounts, or planting decoy pro-government or neutral information (strategies discussed further in Section 3.5.4).

Advice: use secure chat applications 11 participants used or tried to use Telegram, with several mentioning its privacy properties ("*more private than WhatsApp and Facebook*" (P8)). 4 participants mentioned Telegram's encrypted messages and capacity for self-deleting messages (P5, P11, P12, P13).

During the course of the interviews, 4 participants were familiar with the app "Signal," but one of them (and potentially two more) referred to it as a (buggy) app that had offline messaging capabilities (P6, P12, P14). We learned towards the end of the interviews that there is an offline messaging application called *Signal Offline Messenger*[2] that is distinct from *Signal Private Messenger*,[3] the secure messaging app that is relatively common in the US and Europe. Thus, the external advice to use "Signal" may have been misconstrued.

Advice: add foreign phone number as 2FA P5, who attended a formal workshop run by activists, received advice to both add a foreign 2FA number to Twitter and to use VoIP and internet chat apps over regular telephone calls and SMS. P13, a technical expert, advised people to add a foreign number as 2FA. 7 other participants used a foreign number for 2FA.

Less common advice: passwords, misinformation Advice that might seem more general and familiar to the security community was less common. P12, a technical expert,

[2] `play.google.com/store/apps/details?id=com.raxis.signalapp`

[3] `play.google.com/store/apps/details?id=org.thoughtcrime.securesms`

said, "*A group of IT professionals had an account where they posted such advice... change your passwords regularly, make sure it contains letters, names, numbers, unique characters, etc...*" However, only one participant mentioned changing passwords.

Similarly, P3, a fact checking expert, was part of an effort creating and sharing infographics "*to educate the wide public about how to verify news..., how to read the news, how to verify the claims, how to verify any anybody's photos using Google image application.*" However, no participant mentioned receiving specific advice on dealing with misinformation.

Comparison to general-purpose advice Stepping back, we observe that the advice given to (and among) Sudanese activist does not directly echo common general-purpose security advice given by the US- and Europe-based technical communities, other than the general advice to use secure chat apps (which, as discussed in Sections 3.5.3 and 3.7.1, was not always actionable). For example, the most common expert security practices in Busse et al [42] are to update regularly, use password managers, 2FA, ad blockers, while the most common non-expert security practices are using antivirus software, creating strong passwords, and not sharing private info. Of the expert behaviors in [42], participants only mentioned using 2FA, with modified advice: use *foreign* 2FA (discussed in Section 3.6.1). Outside the academic community, there has also been mixed advice and debate about whether WhatsApp should be considered safe by activists [297, 302].

Comparison to worldwide activist advice Through an anecdotal (news and social media as of September 2020) view of US Black Lives Matter (BLM) protesters and Hong Kong protesters, we observe that despite the different adversaries and political goals, there are important overlaps in advice and also significant differences. For example, protesters in Hong Kong are concerned about facial recognition, so they wear both facial masks and a black T-shirt [202]. Though our participants talked about physical security, and one suggested that anyone who was taking on the risky role of livestreaming should not wear bright colors so as to not stand out (P7), they did not adopt defenses against facial recognition or video surveillance, likely because they did not believe the Sudanese government was capable of it (P1, P5).

In a recent article, BLM protestors were advised to carry burner phones, but, if they cannot, the article advised protesters on a variety of preparatory tasks in anticipation of an adversarially-controlled network (e.g. IMSI catchers / Stingrays) and physical seizure of device (but still subject to US laws, which protect most from being forced to give up their passcode, unlike in Sudan)—for example: download Signal, change location permissions on their phones, back up and encrypt their phones, use a passcode instead of biometric authentication, write contacts on your body [311]. While the same high level concerns applied to Sudanese protesters, they were advised to use significantly different tactics, revealing that while advice can follow a certain high level framework to enumerate adversarial concerns (Section 3.6), protesters in different countries require very different *concrete* advice.

3.6 Political influences on the technical defensive landscape and activist threat model

Here we examine the key political factors in pre-revolution Sudan that shaped activists' defensive strategies.

3.6.1 International politics dictate available apps and features

US sanctions on Sudan mean that mobile users in Sudan do not have access to all apps or app features. Through this subsection, we explore these restrictions, and find that the influence of international politics makes it challenging to create security and privacy recommendations that fit multiple vulnerable user groups, since different groups have access to different applications and features.

Restrictions on download and on 2FA Due to the US sanctions on Sudan, the entire iOS app store is inaccessible without a VPN (P11) [65, 308]. P11 described how users in Sudan download iOS apps: "*You either get a VPN on your laptop and download things, and* *then get a VPN on the phone... but sometimes it doesn't work and it's a whole process. Or when you buy a new phone, you just have the store download everything for you. A lot of people do that. My dad does that all the time, and we end up with the store's Apple ID.*" Sharing Apple IDs may impede users' privacy, and an indirect download, or a download from a non-official app store, raises questions of app authenticity. Additionally, people in Sudan cannot directly pay for apps or app features due to the economic sanctions, so apps with paid security or privacy features, or security and privacy-focused apps that are not free, are not easily accessible. Sanctions also mean that Sudanese domestic phone numbers are not accepted as a second factor of authentication (2FA) "*because in Sudan Twitter does not have verification for Sudanese numbers*" (P1).

3.6.2 Technical capabilities of nations supporting Sudan

Activists' perception of foreign capabilities and their ties to technology companies drives their threat models and tech use. The perceived technical capabilities of foreign governments that supported Elbashir's regime—e.g., Saudi Arabia and the United Arab Emirates—were a driving factor in some participants' threat models. P12 reasoned that the Sudanese government could have the same access to information from social media companies as wealthier countries: "*there were cases in Saudi Arabia where...the Saudi Arabian government would purchase information.... So there was this possibility that the government of Sudan was able to purchase such information from Facebook.*"

In addition, our participants' mistrust in Sudan's supporters extended to the foreign SIM cards they were comfortable using. P5 believed the Saudi government could acquire specific user data on behalf of Elbashir's regime through monetary influence and that they would pay Twitter to extract information about Sudanese users who had Saudi SIM cards: "*the Saudi government has shares on Twitter, so we are not very trustful... [there is] sharing between Twitter and the [Saudi] government, so your number should not be a Saudi number. It has to be something in Europe, for example*" (P5).

The perception that privacy on social media was only as good as the money paid by a government, in combination with the lack of choices in apps, led some to feel a lack of control or sufficiency. Asked whether people continued to use Facebook despite the possibility that the Sudanese government could purchase information, P12 said: "*there wasn't any other solution. We reached a phase where we were saying 'what is the worst that could happen.' People have died because of this.*" We cannot address the accuracy of P12's perception about the availability of Facebook data to the Sudanese government, but we do note that according to Facebook's public log of government requests, during January-July 2019 there were 15 requests by the Sudanese government for information on 23 user accounts, and the following period, for the latter half of 2019, had 52 requests. According to Facebook, they did not produce information in response to any of the requests.[4]

3.6.3 The power of the state to compel authentication

Sudanese authorities obtained arrestees' phone passcodes or biometrics in order to search their phones for anti-government activities and proof of activism or identity, a major threat for all participants. P11 explained the threat of legal (or legally unquestioned) violence at the start of the revolution: "*are they going to be killing people, or just torturing them, or just beating them? We had no idea the extent of the brutality.*"

P12 detailed the threat of physical device seizure: "*the security services would look into WhatsApp first, then Facebook. They would look into your latest posts and then they would say that this person has a history of anti-government posts.*" In recounting their arrest, P9 described that they were so confident in their defenses that they wrote down their passcode for the police: "*The first thing they told me, they told me to 'open your phone.' And I just told them, 'give me a pen and paper, I will write it down for you. So whenever you want to open my phone, you just open it.*" We explored P9's defensive strategies earlier throughout Section 3.5, but P9's confidence was not unwarranted: per their telling, they were detained for 7 days, all through which the police had access to their phone, and the police were never

[4] Requests for Facebook data (Sudanese government): `https://govtrequests.facebook.com/government-data-requests/country/SD/jul-dec-2019`

able to prove P9's identity as an activist because of P9's low tech but meticulous defenses.

P5 knew someone who used biometric authentication to ensure plausible deniability upon arrest by using someone else's fingerprint to lock their phone, taking advantage of their knowledge of the adversary's legal power: "*One of them was a high ranking activist on the security people's sheets, and they were threatening [them] by telling [them], 'if you don't open your phone' because [they] used fingerprint, but [they] used someone else's fingerprint! So they couldn't open it.*"

3.6.4 Government control over the telecom infrastructure

The goverment's control over the telecommunication infrastructure shaped activists' threat model and drove adoption of technology. 12 participants believed that the Sudanese government could surveil their communications through a combination of control over the telecommunications infrastructure, influence over ISPs, and technical exploitation. P1 explained their perception of the government's surveillance capabilities, tying together the threat of arrest with the threat of surveillance: "*they can tap your phones for sure, like your phone calls and SMSes...but...they have to know who you are or which number is yours.... But if they got your phone, like if you got arrested and they got your phone, then they're definitely going to keep tabs on you if they release you after.*" P1's perspective points to the difference between surveillance and mass surveillance: some felt comfortable using mainstream applications—even SMS, during the blackout—if they did not already believe they were specifically targeted, as mentioned earlier in Section 3.5.

P13, a technically experienced activist, explained how the threat of the government's influence over telecommunication companies led to incidents of people being locked out of their social media accounts: "*They can only do this using the old stupid way. For example on Facebook, I forgot my password and then they would enter the number and then they would get the code as they already have access to telecom companies. They would get the code and reset the password and then they would lock you out of your account.*"

In addition to surveillance, activists contended with censorship and blackout: during the revolution, the government initially curtailed social media access for roughly 10 weeks, and later imposed a complete mobile data blackout[5] after the June 3 Khartoum massacre. Both required people to find alternate communication solutions.

Some anticipated the censorship and tried to prepare: "*we expected a digital shutdown ... it happened in 2013, a complete shutdown. And I also lived through the Egyptian revolution, so I also saw that happening there, albeit it was way shorter*" (P11). To prepare for a social media blockade that could expand to include the Google Play store, P13 developed a news dissemination app that was never uploaded to the store and could only be shared via Bluetooth, "*I was honestly expecting that they would block play stores, Google Play store and the others with VPNs. Because when they blocked VPNs I thought they will block the actual store because it's natural—you blocked this VPN, I will download another one.*"

3.7 Societal context enables adoption

Now we turn to the social characteristics of the Sudanese activist community that both supported and hindered technological adoption.

3.7.1 Operating at the lowest common denominator of the group's digital and security literacy

Activists' practices are shaped by their own knowledge of technology, as well as others' digital and security literacy, because the security of the group depends on the security of every member. We find that differences in digital literacy between activists that needed to communicate with each other may have resulted in less secure behaviors by *all* parties. P11 explained that digital literacy is a barrier to secure practices: "*that's one of the key issues of Sudan, that people really don't have digital literacy, or digital security literacy.*"

P3 and P13, experienced activists, adjusted their technology use and advice to align with the technology use of the greater group. P3 was forced to use WhatsApp instead of

[5] Most people do not have regular access to home internet; thus, a mobile data blackout is effectively an internet blackout for most people

Signal, which they perceived to be less secure because "*WhatsApp might be monitored by the security forces in Sudan.*" P3 explained: "*For example if you need to reach out to an activist on the ground, some of them do not have the background how to use Signal... They might lack that technical ability to use these secure applications. So that's why we said, okay, we can use WhatsApp, but without going into details.*" P13 chose not to ask their colleagues to adopt Telegram, a new app, because even if they did use the app, "*they will use it without making use of the main feature of self-destroying messages. And this way there isn't any reaped benefit.*"

P9, also an experienced activist, explained that others' digital literacy prevented their own adoption of new chat apps because they needed to be confident their colleagues could use the app correctly: "*having a new application, that means that you will need to let those people learn a new application and learn how to do it. But for me, everyone knows how to use Twitter, everyone knows how to use Telegram, everyone knows how to use WhatsApp. So I don't have to explain to the person talking to me how to delete a message on WhatsApp. So for me, working with someone through an application they're already using is better than working through another platform.*"

We observe that all of our participants were from the capital of Sudan, and that those outside the capital may have a lower level of of digital literacy, making this issue potentially more pronounced outside urban and developed areas. Because group adoption of technology and security practices is both necessary for group action and group security, the lower level of digital literacy may have had a part in participants' adoption of low tech defensive strategies. More broadly, this finding reveals that digital literacy is a barrier to group adoption and has implications on the design for specific user groups.

3.7.2 Sharing institutional knowledge, including security and privacy advice

We find that activists' social structure supports largely informal sharing of institutional knowledge, including security advice, in line with prior work about security behavior adoption [71, 233, 317], suggesting that a formal education or advertisement campaign for apps targeted at activists might be less successful than leveraging social narratives.

Knowledge sharing through narratives The social structure within the Sudanese activist community supported the informal spread of technical and security advice as institutional knowledge. Although a few gave or received specific technical training, many relied on their friends and more experienced colleagues for security and technical advice through narratives and stories, echoing findings by prior work about security behavior adoption occurring socially [71, 233, 317]. P2 said, "*Most of the advice that I have received were from people around me, for example, from my brother*" or from "*my relative who was in the field [electrical engineering].*" P6, whose neighborhood committee had a resident security expert, taught their friends about both BetterNet, a VPN, and Private Space, a Huawei OS feature that they began using to hide information from the Security Services. P7 said that sharing advice "*with friends and family members... happened a lot,*" and P8 even considered security advice "*a public discourse between young people on how to keep yourself safe.*" P9 also considered such advice "*shared knowledge... I would share the information with my friends and the people who work with me, and they will share it with others.*" P12 mentioned information being passed around about "*what people of Burri*[6] *did, so then we can adopt this.*"

Organized training As the revolution continued, some formal training arose. P5 attended a "*security workshop, to carry out your activism without being noticed by the security people ... It was in someone's house, and there were handouts. So you get the training and then you're asked to spread the knowledge to the people you trust.*" They said they were invited to the workshop because "*[the more experienced activists] started seeing me as someone who was contributing to the revolution.*" Experienced activists also created infographics on social media with security or privacy advice, (literally) relying on social networks to share the advice (P2, P3, P5, P10, P14). In addition, P13 (a technically-savvy activist) taught

[6] Burri is a neighborhood in Khartoum where many of the protests occurred and it was considered the fulcrum of the anti-government uprising

journalists how to use encrypted emails: "*For example there were journalists who wanted to send things but they're usually afraid of sending it via email because of being intercepted. So there was PGP that we taught people how to use. We taught this to close people whom we could meet face to face. We taught them how to encrypt a message to the entity they want to send it to, they enter its fingerprint. And this way they're sure that no one could intercept the content of this message.*"

A core group of experienced members Experience amongst activists is a continuum: some have been activists for years, and others became activists at the start of the revolution. The more experienced activists in our participant pool agreed that in Sudan, experienced activists are a small, tight-knit group, enabling a free and informal flow of information between experienced activists that can then be spread further out of the core of the community. P3 explained: "*The activists who are active in Sudanese politics...they all know each other.... It's not like in the US or Europe. It's a very small community...there is a nickname, the 1000 person.*[7] *The 1000 person, it's kind of a joke, there is 1000 activists in Sudan who are mobilizing everything.*" The small community of experienced activists also supported the existence of institutional knowledge about how to protest more generally (P7, P8, P11). P7 said: "*there are some protest skills that have been developed throughout the years. From 2013*[8] *to 2018, we have developed a lot of skills about how to make a successful protest, how to make it safer, how to document it, and send it safely, and so on.*"

3.7.3 Building trust in a constantly mutating group

As activists' groups are constantly changing with members joining and leaving, there was a continuous need to build and maintain trust in a challenging environment rife with threats: "*We can't really trust everyone, and on the other hand we still have to trust other people so*

[7] P3 used the Arabic term أَلف نَاس. By our interpretation of their words, P3 would not have considered all of our participants activists—they meant 1000 *core*, experienced, dedicated activists, who are connected to each other.

[8] Sudan's Arab Spring protests took place in 2013.

we can work together" (P1).

Root of trust: in person Activists did not rely on technology to build trust both in in-person neighborhood committees and chat groups, with the ultimate root of trust being an in-person meeting or a prior personal relationship (8 participants). Sometimes, activists used social media profiles as part of a "background check," but they did not have one single technology that they relied on for trust building, again, a theme of non-technical or low-tech approaches that are strengths *because* they decrease the technical attack surface (though it could be vulnerable to human intelligence infiltration).

P7 and P8 also spoke about the importance of physically meeting someone new before adding them to sensitive chat groups: "*That's what [P8] said, people have to sit down before, on the ground, and meet in meetings. And of course, if someone from my secure circles added me to a WhatsApp group...it depends also to what extent do you trust the other person who is adding you.*"

P1 described camouflaging trust building activities through street cleaning campaigns, which served as a way to meet in a natural environment and figure out who was trustworthy: "*So every other week, we go out and clean the streets, as to reflect that the protests are peaceful, and this is what we are actually trying to do, not just causing riots—we're actually trying to build the country and make it a better environment for everyone to live at. So at that time, when we did those, we sent public broadcasts to everyone who is willing to join, they can join, and then we follow up from there after we meet them and see if we can actually add them to our group.*"

Bootstrapping trust Participants also relied on trusted contacts to add their own trusted contacts to the group or network, or to gain trust for themselves or their online presence (P1, P7, P8, P9, P10, P12). P1's neighborhood committee's Twitter page, seeking to be a source of news and grow in size, got a friend of a friend who was active and verified on Twitter to post that "*this is not a fake page or anything like that*," which resulted in their

Twitter followers increasing from 50 to nearly 4,000. P9 stated that the practice of the SPA (a trusted entity) "verifying" neighborhood committee social media accounts was common. Boostrapping was also used for building in-person trust: P1 described that new neighborhood committee members were mainly "*mutuals who were already recruited trusted people,*" who were additionally vetted through the street cleaning campaigns described above.

3.7.4 Support from abroad

The Sudanese diaspora performed many roles throughout the revolution, including sending mass text messages to help organize and spread news about protests (P3, P5, P12), disseminating news from inside Sudan to both families and the international mass media (P5, P8, P10, P11), acting as backup communicators or coordinators in case those in Sudan were arrested (P9), factchecking on social media (P10, P11, P12) (Section 3.5.1), and using their own phone numbers as 2FA for those in Sudan (P8, P10, P12) (Section 3.6.1).

Experienced activists in the diaspora were also important to the flow of security and technical advice, as they were exposed to a different set of tools and may have had connections to activists in their country of residence. P3, part of the diaspora, described the connections the diaspora may have, and recounted how their own use of Signal stemmed from a friend who introduced Signal to many colleagues: "*some activists... have connections with European and American activists. Some of them even come from the IT background...[which is] one of the main reasons that they are well introduced to Signal and other applications.... I had a friend of mine who majored in computer science and was a known activist in Sudan. He wrote so many times about similar applications.... The people I know, they're using it because of this.*"

The activist social structure even extended to activists of other nationalities who may pass knowledge amongst a global network of activists. P12 recounted that Signal was suggested by an Eastern European activist group that was "*in touch with our activists giving advice like it's better to use Signal.*" However, P12 went on to say that "*I don't think these calls [to use Signal] found a listening ear,*" revealing, again, the need for the advice-givers to understand the political and societal constraints of each specific community.

3.8 Discussion and Conclusions

Activists' use of technology through political change shows that technology can be democratizing; however, technology can also be a tool of oppression. The burden to build tools that will protect communities from oppression lies on the shoulders of developers, technologists, and policy makers.

Throughout our results, we have surfaced a number of key design principles and tensions, and we have explored how these principles and tensions are influenced by our participants' political and societal context. We encourage future researchers and designers to consider these tensions, sampled here, and to continue to work to reveal further ones:

- In Section 3.5.3, we explore the difficulties that activists faced to adopt new mesh networking apps during the blackout, instead adapting their technology use by falling back on other methods like SMS and telephone calls. The lack of mainstream app support for a robust connection might suggest that certain populations would benefit from mainstream apps including a mesh networking mode; however, this suggestion is in tension with the finding from Section 3.6.2 that activists and others might prefer non-mainstream apps that they perceive to have no ties to governments.

- In the US, domestic arrestees are protected by the 5th Amendment from being compelled to give a passcode [139]. Android and iOS support American users by providing a quick way to force passcode authentication over biometric authentication [200]. However, in Sudan, and in any other country in which authorities can compel detainees to give up their passcode, this design offers no protection, driving Sudanese users to manually sanitize their phones. This costs them time, access to information or contacts, and puts them at risk if they are unable to sanitize their device properly.

- Many of the activists' defensive strategies were low tech, e.g., manually timestamping videos, or deleting texts. These strategies were sufficient, and we observe that the *variety* of the low tech strategies (which were usable because they were low tech) is a great strength of the movement as a whole. However, as technologists, we also observe that many of the strategies did not scale and left the activists open to technical exploitation, if the adversary had had the resources. Thus, we observe a fundamental tension between low tech strategies that are widely usable and provide security in practice, and cryptographically secure technologies or strategies that invite the adversary to focus their resources on technical exploitation and additionally may come with issues of usability and adoption.

Thus, to guide future researchers, technologists, and policy makers in expanding upon, solving, and continuing to discover key design tensions and principles, we build upon our results and present a set of example questions as a guide for understanding the security and privacy behaviors of populations around the world, particularly those facing political strife or those whose membership is mutating—for example, other activists (e.g., anti-racism groups in the US like Black Lives Matter, protesters in Hong Kong), internally displaced or persecuted groups, populations living in warzones, refugees, or non-governmental organizations. Due to the complex nature of politics and society, these are not all-encompassing; other researchers may discover further key issues to investigate.

In order to examine, anticipate, and understand the privacy and security behavior and needs of a population under political strife, it is important to first understand the political situation, both internationally and domestically:

- How does the legal structure define the right to technical and physical privacy? What power does it grant to the governing entity and law enforcement?

- To what extent does the government have control over or insight into the telecommunications infrastructure and industry? Are there any legal or technical restrictions? Is there a history of censorship or internet blackout?

- What foreign powers are allies or enemies with this nation and what are their technical capabilities? Are there any international sanctions and what do they restrict?

Additionally, examine societal characteristics:

- What is the baseline digital and security literacy?
- How does knowledge sharing take place within the group? How do members create trust?
- What is "common security knowledge" within the group?

Given the above, explore how technology responds to a number of hard technical challenges and how users adapt either the technology or their behaviors to fulfill their threat models, or whether their threat models are sufficed. Are their adoptions or adaptations sufficient from a security expert's point of view? Consider the hard technological problems presented in Section 3.5: misinformation; physical device security; and confidentiality, integrity, and availability over an adversarially controlled network.

Such structured questions uncover *fundamental tensions* and *design principles* that may benefit further user groups (e.g., a robust connection through a mesh networking mode, device sanitization on demand or with an emergency-triggered authentication). We observe that the generalization of design recommendations often runs into fundamental tensions, and we encourage designers and researchers to consider how these fundamental tensions can drive innovative solutions, and, in contrast, how design principles might lead to fundamental tensions, in part by asking: what makes it difficult to generalize this solution for other user groups? What solutions would work for others that would not work for this group?

Finally, we encourage the study of diverse populations worldwide in order to reveal further key factors, tensions, and design principles. Particularly, more work is needed to study, understand, and anticipate how user groups, such as vulnerable ones, are influenced toward different uses of technology, and ultimately, how technology can better support those advocating for fairness and social good.

Dissertation themes: change and vulnerability during political revolution. Specifically with regards to the broader themes of this dissertation, this chapter explores how Sudanese activists faced immense and unknowable change during the 2018-2019 revolution, causing them to adapt their use of technology (theme 1), and that their goals of political change directly competed with their need for safety and privacy (theme 2). We also found that activists' technology use was driven by political and social context, e.g., international sanctions, and that design misalignments caused activists to develop workarounds that worked for them but might not have withstood an adversary with stronger technical capabilities (theme 3). Taken together, this chapter contributes an understanding of how software design is a political endeavour, and how designs that do not take into account a population's specific cultural and political context can disadvantage that population, especially when they face increased threats and risks due to change.

Acknowledgements

We thank Ayden Baily, Kaiming Cheng, Yousif Dafalla, Theo Gregersen, Maggie Jiang, David Kohlbrenner, Karl Koscher, Kentrell Owens, Franziska Roesner, Alison Simko, Anna Kornfeld Simpson, Miranda Wei, Karl Weintraub, Yasir Zaidan, and Eric Zeng for their valuable feedback on a draft of our paper. We are also very grateful to Tobias Fiebig for shepherding this paper, and to our anonymous reviewers for their thoughtful and constructive criticism, which made this paper much better.

This work was supported in part by the U.S. NSF under Awards 1565252 and 1915824 and the UW Tech Policy Lab, which receives support from: the William and Flora Hewlett Foundation, the John D. and Catherine T. MacArthur Foundation, Microsoft, the Pierre and Pamela Omidyar Fund at the Silicon Valley Community Foundation.

Chapter 4

COVID-19 CONTACT TRACING AND PRIVACY: A LONGITUDINAL STUDY OF PUBLIC OPINION

This chapter presents my work on the public's views on contact tracing apps from April 2020-November 2020. I explore how the changes during the Covid-19 pandemic—increased health risks, lifestyle changes, new technologies—caused people to reason about security and privacy as a factor when deciding whether to use a contact tracing app. First, I delve into the three themes about change and vulnerability, and then present the research.

Change: a global pandemic. March 2020 began a new era of life for many, as Covid-19 spread rapidly outside China and many regions entered some version of enforced or highly recommended personal isolation ("lockdown") to stem the spread of the virus. Many people's **daily routines changed dramatically**, by working from home, having school-aged children at home, traveling less—or the **health risks** of continuing to do their jobs and conduct their lives increased [58]. The rate of **unemployment** also increased substantially [169], and **financial hardship** and **anxiety** about all of the above and more were common.

Theme (1): new risks, new technologies, a changed lifestyle. The new and (for most) sudden lifestyle changes brought new technologies and new risks, including, to state the obvious, **health risks**, a major strain on healthcare systems, **financial insecurity** for many, and new or changed social mores about physical interaction. With the rapidly changing state of public and personal health, people turned to technology as a tool to reduce further changes to daily routine while mitigating health risks, e.g, by working and socializing from home. **Video conferencing tools**, e.g., Zoom, became ubiquitous[315], and **contact tracing apps** (the subject of this chapter) also came to the forefront of public discussion and opinion, promising to be an answer to the arduous process of manual contact tracing during a pandemic, and stared becoming available in many countries in the summer of 2020. However, **new technologies present new security risks**; indeed, multiple security flaws have been discovered in Zoom [315] and in deployed contact tracing apps [289]. Additionally, we found that many **users had inaccurate and incomplete technical mental models** about how contact tracing apps worked (e.g., they thought that the system designed by Apple and Google explicitly tracked location), leading them to not download the apps. This is a failure of user education with this new technology; while users should not be expected to deeply understand the cryptographic protocols used, they *should* have an appropriate high-level and accurate understanding of data collection, storage, transmission, and sharing in order to make an informed decision.

Theme (2): weighing digital security against physical security and health. We found that when deciding whether to download a contact tracing app, individuals weighed security and privacy against the potential health benefits of the app (for both them and their community), and also considered accuracy and developer competence. This decision shows that **perceptions of digital security and privacy had a direct effect on public health**. Some users may prioritize security and privacy and decline to use a contact tracing app, while others may use a contact tracing app for their or others' benefit despite having privacy and security concerns. There are also reasons other than security and privacy concerns that drive users from contact tracing apps, such as concerns about battery life [159] and efficacy. Additionally, these concerns may be the result of inaccurate beliefs, as discussed above, and users may be making a false choice.

Theme (3): a (missed?) opportunity to design for vulnerable populations. We found that when considering whether to use a contact tracing app, participants thought about the **potential for surveillance and harm to marginalized communities**. Recent work in the usable security community, including some of my own, has explored how marginalized communities have not only *specific* needs, but how the needs of different communities are at times in tension with each other [66, 316]. Contact tracing apps present(ed) an interesting opportunity to design an app—and corresponding user education—that does *not* have to be universally usable (though there still may be groups with competing needs within a region that uses a single contact tracing app). This question—**to what extent do existing contact tracing apps serve marginalized populations' usability, security, and privacy needs?**—is out of scope for this chapter, which is about public *opinion* of contact tracing apps, but I include it as a thought experiment about the idea of universal design and this somewhat unusual class of apps that are specifically not meant for global adoption. Regardless of the *actual* design of these apps, our work shows that participants were concerned about harm to marginalized populations from surveillance from contact tracing apps. The **Covid-19 pandemic has affected marginalized communities more severely due to historical and systemic inequities** [158], so the failure to explicitly protect marginalized communities (including through user education) harms them further.

Co-authors and original publication. This remaining pieces of this chapter were published in ACM DTRAP's Special Issue [270]. In this chapter, I use "we" to represent the work and writing done by my coauthors, Jack Lucas Chang, Maggie Jiang, Ryan Calo, Franziska Roesner, and Tadayoshi Kohno.

4.1 Introduction

Technology companies, university research groups, and governments have been diligently working to deploy COVID-19 contact tracing apps, for which adoption has been slow [51, 72]. Prior work has determined that contact tracing apps are most effective when used by the majority of a population [80, 87, 219]; however, some have raised security and privacy concerns (e.g., [63, 280]) as well as broader concerns about efficacy (e.g., [279]).

Our research seeks to provide to the scientific, technology, and policy communities an informed understanding of the public's values, concerns, and opinions about the use of automated contact tracing technologies. We argue neither for nor against automated contact tracing in this work, but instead we offer a summary of public opinion on potential contact tracing scenarios since many regions have already implemented automated contact tracing programs or are moving towards them. We ask the following research questions:

- **App functionality.** What do potential users want a contact tracing app to do or not do? What data sources do people feel most and least comfortable with being used for contact tracing? Our survey asks about potential app features and multiple data sources, including: location data (e.g., from cell tower data, credit card history, or wearable electronics), proximity data, data from an existing app, and data from a new app by a known entity or company (Sections 4.5.2 and 4.5.4).

- **Developer and stakeholder identity.** What kinds of institutions do potential users trust to conduct or implement automated contact tracing? We ask about trust in a number of potential developers, including government agencies and well known tech companies (Section 4.5.3). We also solicit individuals' opinions regarding contact tracing data being shared with or used by different entities for the purposes of contact tracing. We consider data sharing with and usage by multiple entities, including: their government, cellular provider, cellphone manufacturer, and various well-known technology companies (Sections 4.5.3 and 4.5.4).

- **Changes over time.** How, if at all, has public opinion about the preceding topics changed over time? We discuss longitudinal changes in Sections 4.5.2, 4.5.3, and 4.5.4. We also ask (Section 4.5.5) whether there are any correlations with demographic factors or world events, e.g., the global or regional infection rate.

We capture public opinion using an international paid survey platform (Prolific). Our first survey (April 1, 2020) was repeated weekly through June and fortnightly thereafter, with the latest data collected on November 6, 2020. Each survey collected data from 100 participants, and we collected two surveys in the first week (200 participants total). Our first surveys preceded the initial viral peak infection rate in North America, which was before contact tracing apps were available in many of the regions that now have them, and was early in the public discourse about contact tracing; our later surveys track how public opinion evolves over time.

This chapter addresses a broad audience—researchers, app developers, public health officials, policy makers, etc. Our results can inform (1) ongoing technical efforts to design contact tracing apps in a privacy-preserving manner, (2) how the makers of such a contact tracing app or program communicate the privacy properties of their contact tracing program to their potential users, and (3) legal, ethical and policy discussions about the appropriate use and design of such technologies. At a high level, we find:

- **Privacy preferences are stable over time at a population level.** We find that public opinion about privacy and contact tracing is roughly stable over time, suggesting that our—and others'—results can successfully inform future efforts. We find there is a shrinking population that has yet to use contact tracing apps, and that privacy concerns limit potential users' willingness to download the apps. Therefore, the population that does not yet use a contact tracing app may appear to become more privacy conscious as the less privacy conscious leave it and download an app (Section 4.5.2).

- **An abundance of concerns about data sharing, usage, and developer identity leads to a personal decision about the trade-offs between privacy and health, and leaves no perfect solution.** We observe that potential contact tracing app users care deeply about the identity of the developer, and have strong opinions about with whom data should or should not be shared. However, we note that participants disagree about trusted entities. Many participants raised concerns about sharing with their government and data being used for advertising or government surveillance, now or in the future (Section 4.5.3).

- **Informed consent and transparency about data sharing and usage may mit-**

igate some privacy concerns. Participants expressed a strong desire for meaningful consent and control over their data. If developers and policy makers (1) better inform the public about the current and future use of their data, and (2) give individuals control over how their data are used, they may be more willing to enroll in automated contact tracing. For example, we find support for judicial oversight of government data usage in some circumstances, potentially making users more confident that their data would not be misused (Section 4.5.3).

- **Mental models of technical and legal concepts are often incomplete or inaccurate, but play a significant role in potential users' willingness to begin contact tracing.** Participants repeatedly reasoned about the *accuracy* of certain technical methods of contact tracing (e.g., GPS vs Bluetooth), the *competence* of the app developer to implement contact tracing at a technical level, and the *capability* of their government to protect (or exploit) their data. Through this reasoning, we identified multiple inaccurate or incomplete mental models, e.g., some participants thought a proximity tracking app would be less secure than a location tracking app due to constant communication with others' phones via Bluetooth. Other participants overestimated the prevalence of judicial corruption, causing them to discount the protection potentially provided by judicial oversight of government data usage. These mental models invite stakeholders to improve user education so that users can make well-informed decisions.

4.2 The evolution of contact tracing during the COVID-19 pandemic

In order to contextualize our results, this section captures the state of the world on April 1, 2020, when we first deployed our survey, and how both the infection rates and contact tracing efforts progressed through November, when the last data reported on here was collected.

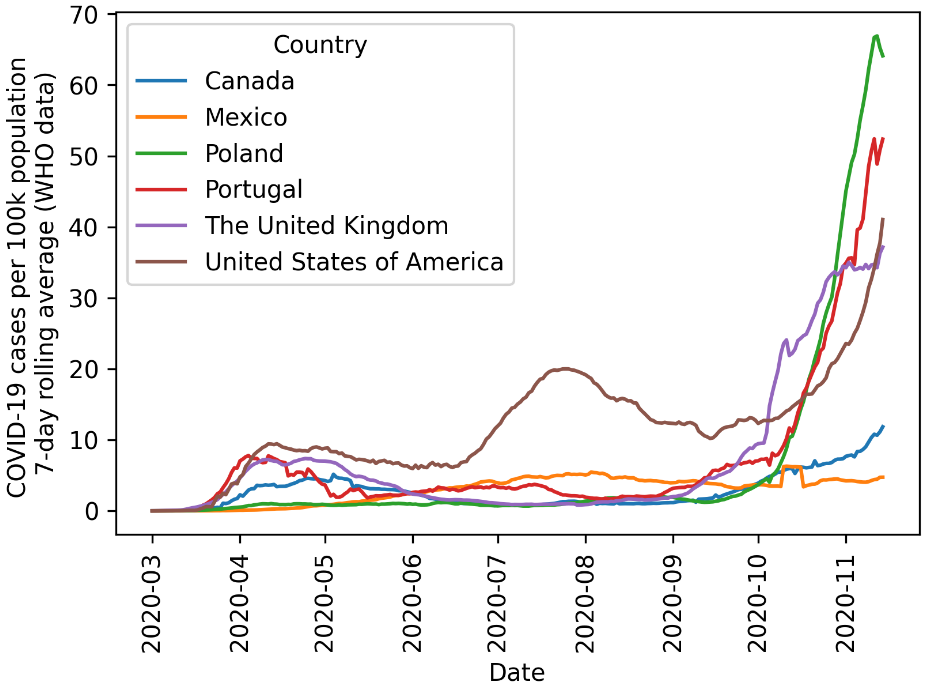


Figure 4.1: COVID-19 new infections per 100k as reported to the World Health Organization (WHO) [221] for the six countries from which we had at least 100 participants (together, these countries comprise 74.4% of our participant pool).

4.2.1 COVID-19 infection rates and quarantine restrictions

Infection rates. On April 1, the course of the COVID-19 pandemic had not yet reached its first peaks outside of Asia. Figure 4.1 shows the number of infections per 100k people in the six countries from which we had at least 100 participants total: Canada, Mexico, Poland, Portugal, the UK, and the US. After an initial spring peak in many countries in our dataset, the rate of infection declined. The US saw a second peak of infection in August, though rates of infection in many others countries remained low [85]. In November, many countries were experiencing skyrocketing infection rates, as seen in Figure 4.1.

Regional lockdowns. On April 1, as we began our survey, many European countries, (e.g., the UK, Germany, Italy, and Spain), were under varying forms of lockdown, with some combination of schools, restaurants, bars, and non-essential shops closed, public gatherings banned, and citizens urged or mandated to stay inside except for essential outings [57, 153, 168, 262]. Many in the US were under similar restrictions, though some states issued no stay-at-home orders at all during those early months [109, 161, 199, 266].

Due to the lower infection rates over the summer, restrictions largely eased in Europe but had been re-implemented in many countries as of November in the form of nightly curfews, closures of non-essential businesses, travel restrictions, and mask-wearing and social distancing mandates [30, 162, 178]. In November, restrictions in many US states were not as strict, with limitations but not bans on indoor activities (such as dining and shopping) and masks mandated in some but not all states [199].

4.2.2 Contact tracing technical efforts and app adoption

Here, we briefly overview existing contact tracing app efforts and their adoption as well as the conversation around how to contact trace in a privacy-preserving way. The purpose of this section is to contextualize our findings and recommendations, not to give a comprehensive look at technology-enabled contact tracing efforts.

Why automated contact tracing? Traditionally, contact tracing is done by a team of public health experts and focuses on tracking down those who might have been infected by someone who tested positive for a disease, in combination with widespread testing. A state, region, or other entity might implement *automated* contact tracing (e.g., to augment or complement human-based efforts, for which there has been a shortage [226, 272]) for multiple reasons, although though not all experts agree that automated contact tracing is needed or will be effective. For example, automated contact tracing might be used to keep infection rates low while allowing people to leave their homes, or used to enforce quarantine for people identified as COVID-19-positive.

Existing automated contact tracing programs. As of April 1, some governments had already deployed automated contact tracing programs using a variety of devices and data sources [322]. For example, contact tracing apps existed in Bahrain, China, Colombia, the

Czech Republic, Ghana, India, Israel, the Republic of North Macedonia, Norway, Singapore, and some US states [2, 28, 56, 111, 127, 148, 151, 188, 203, 212, 213, 299, 309]. Some apps were mandatory (e.g., in China), but most were optional (e.g., in Singapore) and struggled with low adoption [51]. Hong Kong deployed electronic wristbands to those infected with COVID-19 to ensure they did not leave their homes [258]. In South Korea, the government sent text messages with details about new COVID-19 cases and made available a central database with anonymized information; however, some entries were specific enough to be traced back to a single person and initiated damaging rumors [61, 165]. Additionally, Taiwan and Israel both began using cell tower data [127, 143].

On April 10, Google and Apple announced "*a joint effort to enable the use of Bluetooth technology to help governments and health agencies reduce the spread of the virus, with user privacy and security central to the design*" [117]. In May, they released the first version of their Exposure Notification API [41, 53, 83]. The API uses proximity tracking through Bluetooth, is opt-in, and can be used only by public health authorities; Apple and Google report that the data will not be monetized [41, 53]. In September, Apple and Google launched "Exposure Notification Express," allowing users to participate in contact tracing without downloading an app [83].

Since the release of Apple and Google's Exposure Notification API, many public health authorities have released apps using the API. According to the *MIT Technology Review* COVID Tracing Tracker [220], in November, 46 non-US countries were using automated contact tracing applications, 13 with Apple and Google's API and 4 with DP-3T [300]. Additionally, at least 12 US States were using the Apple and Google API in November [251, 323]. Apps have been released steadily over time around the world, yet adoption remains low in most regions: of the apps for which the adoption rate is in the *MIT Technology Review*'s database, as of November, Iceland, Ireland, and Singapore had the highest voluntary adoption rates, at just below 40% of the population of each country [220]. Though automated contact tracing is more effective with more users, it can be effective at low rates of adoption as well [219].

Design decisions affecting security and privacy. Design properties at multiple levels affect user security and privacy, some of which are transparent to users (e.g., being potentially identified as infectious in some designs) and some of which are more opaque (e.g., broadcast vs narrowcast; centralization vs decentralization). For a more complete and in-depth discussion of these properties, see [239, 312].

Some groups explicitly focus on privacy-respecting contact tracing. Each group makes design decisions based on its own threat models and on-the-ground situations, including Apple and Google, the Massachusetts Institute of Technology (MIT), the University of Washington (UW), PEPP-PT, Inria, and DP-3T [43, 117, 149, 252, 300]. One high-level distinction that has become extremely popular since our initial surveys in early April is *proximity tracking*, where a user's phone tracks other nearby phones, rather than a more traditional implementation of location-based contact tracing.

Additionally, other, non-smartphone methods are being used to trace contacts, such as credit card purchase history, facial recognition on surveillance camera footage, and wearable devices [147, 274, 275].

4.3 Related Work

Other groups have also investigated public opinion on location tracking during COVID-19, described below.

Themes: privacy concerns abound, but a majority indicate a willingness to download contact tracing apps. Many groups have assessed a population's willingness to download a contact tracing app, finding rates between 27 and 84% at different points in time, with different privacy and data sharing and usage situations and different populations, including Australia [75, 76, 102], China [171], a number of countries in Western Europe [13, 20, 123, 131, 152, 171, 222, 321, 324], and the US [13, 20, 23, 131, 132, 171, 181, 238, 298, 330]. These works identified concerns thematically similar to ours, such as privacy concerns about sharing with the government, and correlations between willingness to download and COVID-19 concern levels or demographic information, e.g., age.

Cross cultural studies. Some groups have studied participants from multiple countries, including [13, 20]. For example, Altmann et al. found that people in the US and Germany were less likely than people in France, Italy, and the UK to install a contact tracing app due to security and privacy concerns [20]. Kostka and Habich-Sobiegalla compared public acceptance of contact tracing apps in China, Germany, and the US; in line with Altmann et al., they find that participants in Germany and the US were much less accepting of an app than those in China [171].

Longitudinal studies. Garrett et al. are studying public opinion over time in several countries (including Australia, Germany, and the UK) by periodically surveying participants from those countries in "waves" [76]. In Australia, Garrett et al. have found widespread acceptance for contact tracing apps but lower download rates than were predicted by attitudes about contact tracing apps [102].

Situating our work. In the context of existing work, our work adds a *regular and periodic* survey of public opinion, capturing trends and stability over time. Additionally, the free response answers present in our data provide rich insight into the values and concerns underlying individuals' willingness to download, allowing them to express themselves in their own words in addition to via prescribed quantitative options.

4.4 Methodology

To collect rich data and measure public opinion, we designed an approximately 20-minute online survey with both multiple choice and free response questions. Our survey was implemented in Qualtrics. We deployed the survey through Prolific, an online survey platform based in the United Kingdom.

Our institution's IRB determined that our study was exempt from further human subjects review, and we adhered to best practices for ethical human subjects survey research, e.g., we paid at or slightly above minimum wage, all questions were optional except the initial screening questions about age and smartphone usage, and we did not collect unnecessary personal information.

4.4.1 Survey Protocol

Because we expected most participants to live in countries where contact tracing apps were not in ubiquitous use, at least for our initial survey, we designed the survey to elicit attitudes about contact tracing in specific *hypothetical* situations. The survey did include branches for those who had already downloaded an app for tracking or mitigating COVID-19, or who had the opportunity to but chose not to, but here, *we focus on those who did not have a contact tracing app* at the time of inquiry. To avoid biasing participants towards presenting themselves as more privacy-conscious than they are, the survey did not mention "privacy" until its final two questions (demographics) and asked instead about participants' "comfort" with various situations, or their "likelihood" of downloading an app in a certain situation. Each section (except for demographics) concluded with one or more free-response questions, inviting participants to explain their opinions.

When designing this survey in late March 2020—and adding to it in response to the evolving world—we paid close attention to the ways that technology and terminology might change, opting to describe terms that may fall in or out of style (like "contact tracing" or "exposure notification") and prioritized longitudinal consistency by not editing questions after they had appeared once (other than to correct the rare typo). We expand on this experience of future-proofing a longitudinal survey during a rapidly evolving event in Section 4.6.

The survey had the following main sections (excluding questions for participants who were already using a contact tracing app). See Appendix B.1 for the full protocol.

Demographics. We asked participants three types of demographic questions that focused variables we hypothesized might correlate with their attitude towards COVID-19 and contact tracing programs: (1) standard demographic questions, like age, gender, geographic location; (2) general political views, news sources, and privacy and technology interest and knowledge; (3) COVID-19-specific questions, like their general level of concern about the pandemic, whether they live with someone who is in a high-risk group, whether they had had COVID-19 or had ever been tested, and their beliefs about social distancing and mask wearing. We asked many of the demographic questions at the end of the survey to help mitigate stereotype threat.

Cell tower location data. We asked participants how comfortable they were with their cell phone manufacturer or cellular carrier using their location data for the purposes of studying or mitigating the spread of COVID-19. We presented participants with three variations of a situation: their location data being shared with their government; their location data being shared with their government if they tested positive; and their location data being shared publicly if they tested positive.

Existing apps using GPS location data. We asked participants to imagine that "the makers of an existing app on your phone started using your GPS location data to study or mitigate the spread of COVID-19." We chose 3 popular apps from each of 5 categories that we expected would use location data (navigation, social media, messaging, transportation, fitness), for a total of 15 apps. Participants rated their comfort level with each of the 15 apps using their location data for mitigating the spread of COVID-19 on a 5-point Likert scale, with an additional option for "I don't use this app." We then asked two free-response questions about the app that they regularly use that they would *most* trust and the app that they would *least* trust to study or mitigate COVID-19.

New app: perfect privacy. We asked participants to imagine a new app that would track their location for the purposes of mitigating the spread of COVID-19 but that would protect their data perfectly. On 5-point Likert scales, we asked how likely they would be to install the app and how it would change their current behavior.

New app: app makers know location at all times but do not share it. Changing the previous scenario slightly, we asked participants to imagine a new app that would know their location at all times for the purposes of mitigating the spread of COVID-19, but this time the app makers would know their location at all times but would not share this information. We again asked participants how likely they would be to download and use such an app. This time, we asked participants to rate their comfort with each company that made the same popular 15 apps we showed them previously. We expanded this list to include other companies in week 3 of the survey. We also asked about their comfort level with five generic entities making such an app: a university research group, an activist group, an industry startup, your government, and the United Nations.

New app: app makers know location at all times and share data with your government if you are diagnosed with COVID-19. Again changing the previous scenarios, we asked participants about a situation in which the new app's makers share their location history with the government if they test positive for COVID-19. We asked, again, how likely they would be to download such an app as well as their download likelihood in two variant situations: if the data were shared regardless of whether they tested positive, and if the government's use of the data were supervised by a judge.

Non-smartphone location data sources. In response to an evolving conversation about alternate data sources, we asked participants next about their comfort level with having location history derived from surveillance camera footage and credit card purchase history (added in week 3). Beginning in week 16, we also asked participants about their comfort with public area sensors or electronic bracelets.

New app: proximity tracking. Due to the growing discussions about and technical work on proximity tracking protocols and apps after April 1, in week 3 we added a group of questions about proximity tracking. We asked about proximity tracking by phone manufacturers, phone operating systems, a new app, and apps from several well known companies or generic entities.

Government use of location or proximity data. In this section, we stepped back from scenarios about specific data sources to ask participants questions about a scenario in which their government acquires their location or proximity data for studying and mitigating COVID-19. We asked about their confidence in their government's deletion of the data post-pandemic, use of data only for COVID-19 tracking, and their general level of concern about their "personal safety or the safety of those in their community."

Desired features in a new COVID-19 mitigation app. We then asked participants about a wide variety of features that a potential new COVID-19 mitigation app might have when notifying people of potential infections or enforcing isolation; features were drawn from existing contract tracing apps or programs. For example, one feature we asked about would "notify you if you came close to someone who later tested positive for COVID-19," while another would "automatically notify the authorities if people were not isolating as mandated."

Location sharing with their government pre-pandemic. Finally, we asked participants to rate their level of comfort with their location data being shared with their government in October 2019, i.e., before COVID-19. Since participants may not accurately recall their own previous beliefs or may have been primed towards privacy-sensitivity by the rest of the survey. Therefore, any results from this data must be treated with caution.

4.4.2 Recruitment

We recruited participants through Prolific, an online survey platform, with no demographic restrictions, since Prolific already requires that all participants be 18 or older. The first questions of our survey screened participants as required by our IRB. We asked: (1) are you at least 18 years old? and (2) do you use a smartphone regularly? If participants answered 'Yes' to both, they proceeded to the rest of the survey.

We ran the survey on Prolific on April 1, 3, 8, 10, and every Friday thereafter until June 5, then every *other* Friday, around the same time (3pm PST). We excluded anyone who had taken any previous version of the survey.

4.4.3 Analysis

In this report, we present analyses of our qualitative and quantitative data. We conducted exploratory and descriptive statistical analysis of our quantitative data rather than testing specific hypotheses, described below.

Longitudinal analysis. To explore longitudinal trends, we present data with time on the x axis and the percent of participants on the y axis. We draw slopes that are statistically significant with $p <= .05$, a standard threshold for significance, but we observe that a statistically significant slope does not necessarily mean that the slope has practical significance. We calculate the statistical mean (μ) for each question.

Demographic analysis. For the questions that displayed longitudinal stability (the majority of the questions), we examined demographic trends by collapsing all weeks of data into one pool. We analyzed each question by: country or region, age bracket, gender, and phone manufacturer, including only demographic groups for which there were at least 100 participants.

Qualitative analysis. To understand participants' values and concerns more deeply, we conducted qualitative analysis of the optional free response questions accompanying many of the survey sections. To analyze these questions, two researchers iteratively created independent qualitative codebooks for each question, first open coding and then creating axial and hierarchical codes for each question. We opted to use separate codebooks for every question except questions that were variants in order to allow the themes from one question to arise independently from the themes in another. When reporting qualitative data, we report the number of participants for each theme, idea, or concept, and attribute quotes to participants using an identifier with both the week and a participant number, e.g., W3P40 for participant 40 from week 3.[1]

4.4.4 Limitations

As Covid-19 quickly became prevalent outside China in March 2020, we tried to both develop a survey as quickly as possible in order to collect early data, and to develop a survey whose questions and wordings would withstand a year of immense and unknowable change. In doing so, we made choices that contributed to both the strengths and weaknesses of this work. In the interest of consistency, we decided to never edit questions other than to fix typos. This decision allowed us to compare data across the entire year of our data collection,

[1] Though each survey had 100 participants, some participant numbers may be greater than 100; we combine results from the two surveys in week 1, so there were 200 participants in week 1. Additionally, some weeks had a few participants who were screened out, causing us to recruit slightly more than 100 participants, and causing some participant numbers to be greater than 100.

but it also means that we did not correct the survey's imperfections—either places where we accidentally did not adhere to survey best practices, or places where the changing world lead to potentially outdated terminology or questions.

Because of our commitment to consistency, we chose not to use the term "contact tracing" in the survey even after we perceived it became popular and commonplace, and instead described the relevant qualities of a contact tracing app (e.g., describing it as "*an app that tracks your location for the purposes of mitigating the spread of COVID-19*" for questions 50-52 (Appendix B.1.5)). This could have introduced confusion if participants thought we were talking about contact tracing but were confused because we did not use the term directly. However, most participants who answered that they have a contact tracing app (Q25) seem to have understood the question, so we estimate that the confusion was minimal (Section 4.5.2.3).

Another limitation of our work is that we did not randomize question or answer order, which can introduce bias [240]. Additionally, another limitation of a survey such as ours, in which participants are asked about different situations without being able to directly compare them, is that opinions about earlier questions may change given later questions [240].

Additionally, though we intentionally recruited from an international audience, our survey was in English, meaning that those who do not read English are not represented, and some with weaker English skills may have chosen not to complete the free response questions; this could lead to potential biases towards English speakers in the qualitative responses. Although we have an international sample, we did not recruit large numbers of participants from any individual country each week, so our data cannot be used to examine country-level trends *over time*. Additionally, some of our questions, e.g., Q69 and Q42, may be more suited towards a US audience, despite the low rate of US participants in our sample. Thus, answers to those questions should be interpreted with caution.

Prior work on Mechanical Turk participants in the United States, a different survey platform than ours, found, with varied results, that online survey participants may not be representative of the general population [256]. Other studies have examined whether online survey participants' security and privacy knowledge and behavior accurately represent the general public, with varying results [156, 243].

Finally, online surveys have inherent limitations. Participants may experience survey fatigue and click through long matrix questions, giving inaccurate answers in order to finish the survey more quickly. From our qualitative analysis, responses to free response questions seem to be on topic and high quality, indicating a low rate of survey fatigue. Survey fatigue, or lack thereof, may also be affected by the fact that participants were paid and therefore incentivized to finish.

4.5 Results

We now report results from our analysis of both quantitative and qualitative data from weeks 1 (April 1, 2020) through 32 (November 6, 2020) of our survey. On week 1, we conducted two surveys (April 1 and April 3); for weeks 2-10 (through June 5), we surveyed participants once a week; for subsequent weeks, we surveyed every two weeks (hence, there is no data for weeks 11, 13, 15, etc.).

Our survey had two branches, one addressing those who had a contact tracing app and one addressing those who did not. Here, we focus on the latter cohort since they may share concerns and values we must understand in order to make it possible for them to (1) have safe access to automated contact tracing, and (2) be able to make an informed decision about participating.

In Section 4.5.1, we describe our population demographically, finding that while our participants hail from dozens of countries, minority viewpoints may be absent. In Section 4.5.2, we consider estimates of a population's willingness to download a contact tracing app. We also consider how privacy concerns affect willingness. We find that while adoption of contact tracing applications *is* increasing, a significant minority of the population does not intend to use them, and that privacy concerns are indeed a central concern, even amongst those who might download an app. We also consider functionality users might want from contact tracing apps, finding support for bare-bones tracing features but not for more privacy invasive ones, such as quarantine enforcement.

In Section 4.5.3, we examine values and concerns potential app users might share about tech companies, governments, or other entities that develop contact tracing apps. We observe that users have substantial concerns about their data being shared or used without their consent and for purposes that might harm them or others. We also find no one-size-fits-all app developer profile: comfort with an app developer (e.g., Google or the US government) is a complex decision that differs for every user; therefore, policy makers, tech companies, researchers, governments, and public health experts must work together towards protecting users and helping users understand the protections in place so that they can make informed decision. Finally, in Section 4.5.4, we more broadly explore user values and concerns through a discussion of alternative data sources for contact tracing, including cell tower location data, credit card history, public sensors (including surveillance cameras), and wearable electronics. Expanding upon themes from previous sections, we observe that anonymity and technical *accuracy* are of great concern to users, whose mental models may be incomplete or inaccurate.

Two notes on terminology: We use the term 'contact tracing' to include 'location tracking' and 'proximity tracking.' When reporting qualitative results, we use the format W1P100 to mean participant 100 from week 1. Further, our notation Q[N], where N is a number, refers to unique identifiers in the Qualtrics survey platform that we used. Question numbers do not appear strictly in order; we analyze questions in groups but encourage readers to refer to the full survey protocol in Appendix B.1 if necessary. Finally, in longitudinal plots, we draw lines when statistically significant ($p \leq .05$) and show the average (μ) in the legend for all questions.

4.5.1 Participant Demographics: European, male, white, and young

Over the course of 20 surveys and 32 weeks, we reached **2337 participants**, **mostly from Europe**. Countries with at least 10% of participants in our dataset are from the United Kingdom (22.4%), Portugal (15.9%), and Poland (14.6%). 9.9% of our participants were from United States. European countries (including the UK, Portugal, Poland, and 21 others) comprised 73% of total survey participants.

As is common in online surveys [256], participants were **overwhelmingly young**. Over 70% were under the age of 30; 54.9% between ages 18 and 24 (we screened out anyone younger than 18); 18.9% between 25 and 29; and 11.2% between 30 and 34, with a long tail to a highest age bracket of 70-74.

40.7% of participants who disclosed their gender were female; **58.1% were male**. Approximately 1% of participants disclosed that they were transgender, genderfluid, genderqueer, non-binary, or agender. We manually bucketed participants' gender identities as reported in a free response text field; we believe we have stayed true to participants' gender identities when bucketing, though these identities may change over time and our respondents may have included more trans or gender non-conforming participants than disclosed as such. To avoid stereotype threat, we asked most demographic questions at the end of the survey, asking only high-level questions about demographics (e.g., location) and COVID-19 at the start.

In week 12 (June 19), we began collecting data on race and ethnicity. Because race and ethnicity are complex and have different meanings throughout the world, we provided participants with a number of races or ethnicities commonly asked about in surveys [55, 94] and also offered a free response question if they wished to self describe in addition to or instead of options we provided, as recommended by the EU [86]. Of these responses, **79.6% identified as white**, 13.5% as Hispanic or Latinx, 6.9% as Asian, 3.2% as Black or African-American, and less than 1% as American Indian, Alaskan Native, Pacific Islander, or Native Hawaiian. Percentages add up to more than 100 because some participants selected multiple identities. Those who chose to self describe indicated both intersectional identities and European ethnicities, such as Slavic, Irish, and Scandinavian.

Though we have survey participants from a variety of countries, they are overwhelmingly young, white, and European. Thus, our survey is dominated by racial and ethnic majorities in the countries that we surveyed from and, thus, privacy concerns of those who we were unable to reach—**older adults, racial and ethnic minorities—are not well represented in our dataset.**

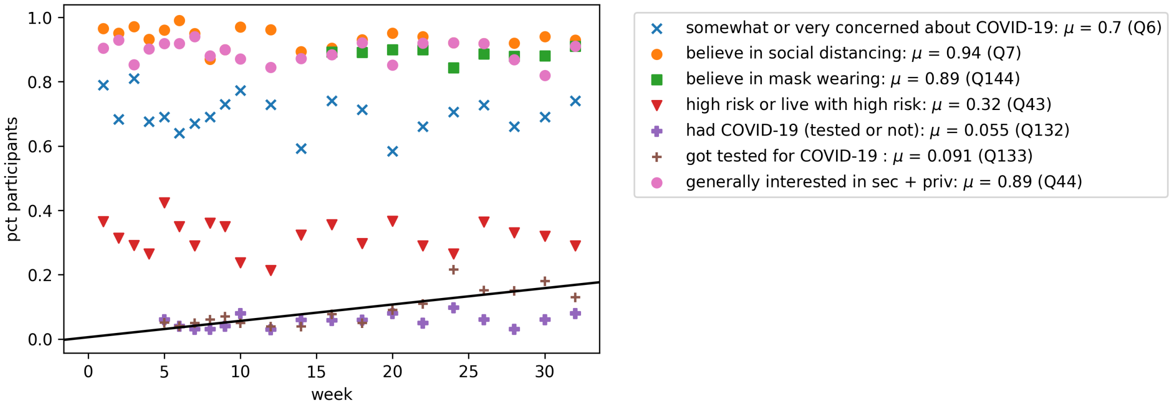


Figure 4.2: This plot describes our participants' attitudes toward COVID-19 and preventative measures. Respondents have a generally high degree of belief in preventative measures, like mask wearing and social distancing. The line at the bottom shows a statistically significant increase in the percent of participants who had been tested for COVID-19.

4.5.1.1 Participants who are concerned about COVID-19 and believe in social distancing and mask wearing

Figure 4.2 summarizes COVID-19-related demographic information about participants, revealing no statistically significant longitudinal trend other than a slight increase in those who were tested for COVID-19 (Q133, $p < .01$). However, our data reveal that our participants are generally concerned about COVID-19 ($\mu = 70\%$) and believe in social distancing ($\mu = 94\%$) and mask wearing ($\mu = 89\%$) as preventative measures for COVID-19. A sizeable minority are in a high risk category or living with someone who is ($\mu = 32\%$).

A report on public attitudes in the US towards mask wearing and other COVID-19 prevention measures found that mask wearing increased substantially between June and August in many regions of the US [173]. We do not see such an increase in support for mask wearing in our data but do find support for such measures similar to higher numbers from [173]; the lack of trend in our data may be explained by our smaller and Euro-centric population. A May 2020 CDC report found that those surveyed in Los Angeles and New

York City overwhelmingly supported mask wearing and social distancing measures [64], with numbers similar to our results. However, as revealed in [173], many US regions showed limited support for mask wearing and other measures: these views are not represented in our data, so our findings must be interpreted carefully to consider those who we did not reach.

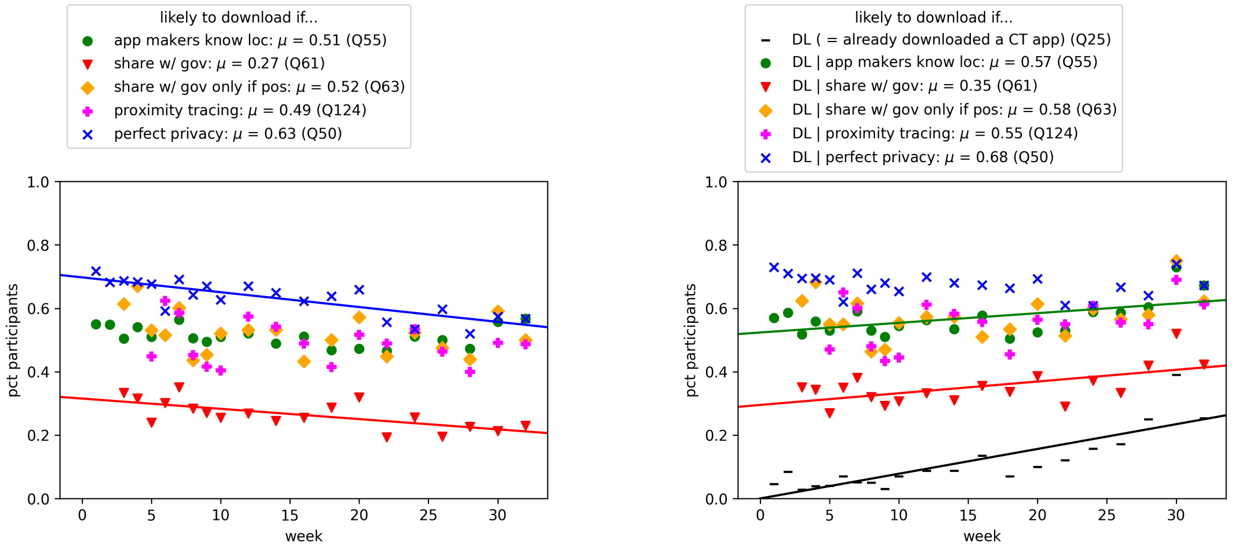
4.5.2 Expectations about app functionality, data sharing, and technical implementation suggest privacy and accuracy concerns influence users' willingness to download contact tracing apps

We now ask what proportion of our population might be willing to download a contact tracing application, and what concerns or values they might have about what the app does. Estimating the number of people willing to download under *some* circumstances is critical to finding the best-case success of voluntarily downloaded contact tracing applications. Understanding potential users' concerns and values will help app makers and public health experts in ongoing efforts to tailor policy, technology, and public awareness campaigns towards reaching global critical mass usage of automated contact tracing. We find that:

- The upper bound of people willing to download a contact tracing app remains roughly constant over time, but potential **users may be becoming more willing to accept an app that does not have perfect privacy** (i.e., an app that shares data under some circumstances) (Sections 4.5.2.1 and 4.5.2.3).

- When comparing contact tracing apps that use location tracking (GPS) and proximity tracking (Bluetooth), participants considered both **expected technical accuracy** and **privacy concerns** (Section 4.5.2.4).

- Participants value a contact tracing app that **notifies them (or others) if they have been exposed to COVID-19, but not an app that would enforce isolation or quarantine** (e.g., [164]), citing concerns about algorithmic inaccuracy and equity. In



(a) This graph addresses the question: what kind of app are those who do not already have a contact tracing app willing to download? One might expect this sector of the population—a shrinking portion—to become proportionally more privacy-conscious over time since those who are less privacy-conscious may download an app voluntarily.

(b) This graph addresses the question: What percent of the population as a whole might have a contact tracing app in the future? (i.e., each colored point is the sum of those who already have a contact tracing app and those who might be willing to download one.)

Figure 4.3: The percent of respondents who indicated that they would be somewhat or extremely likely to download an app that tracked their location or proximity to others “for the sake of tracking or mitigating COVID-19. The left plot (a) shows *only the participants who do not have a contact tracing application.* The right plot (b) shows ***all** participants: each colored point is the* ***sum*** *of those who already have a contact tracing app and those who said would be somewhat or extremely likely to download one.*

qualitative results, participants organically suggested *informational* features, such as regional guidelines or medical advice, perhaps revealing a lack of reliable information about COVID-19 or an unmet desire for a unified or official source (Sections 4.5.2.5).

4.5.2.1 Not everyone intends to download a contact tracing app; data sharing concerns reduce likelihood to download

Figure 4.3a shows that even if a contract tracing app were to "protect your data perfectly," a significant minority of those who have not yet downloaded an app do not intend to voluntarily do so. Approximately 63% said they would be somewhat or extremely likely to download a contact tracing app with perfect privacy, while many fewer would download an app that shared their location with their government ($\mu = 27\%$). Participants showed no significant preference between an app for which the app makers have access to location (Q55), an app for which the developers share data for those who test positive with the government (Q63), or proximity tracking (Q124), all around 50% of those who have not yet downloaded an app.

4.5.2.2 Concerns about sharing data with the government limits willingness to download; users may be more likely to share data if they test positive for COVID-19

Participants were more comfortable with an app that would share location data only from users that tested positive ($\mu = 52\%$) than one that would share location data from all users ($\mu = 27\%$). This difference in comfort reveals that participants have strong concerns about sharing location data with their government and that those concerns may limit their willingness to download a contact tracing app. This difference in opinion also raises questions about participants' mental models of the mechanics of contact tracing—who do they believe is conducting contact tracing?—as well as their views of government data usage (explored further in Section 4.5.3).

More broadly, these results suggest that those who test positive for COVID-19 may be more likely to cede some privacy. W1P194 wrote: "*If I were to be tested positive for the virus, I would definitely sacrifice some of my privacy to the government if it means protecting* *others. However I'm conflicted on the thought of sharing this data with the government if I am healthy.*" W6P58 said: "*I don't want the government to track my location. However, if i tested positive for Covid-19 I understand why it would be necessary so I would reluctantly accept it in that case.*"

4.5.2.3 Not everyone will voluntarily download a contact tracing app

In Figure 4.3b, we add to Figure 4.3a—the participants who have already downloaded a contact tracing app—in order to ask a subtly different question: what percentage of the entire population might have a contact tracing app in the future? We observe, first, that the percent of our participants who have downloaded a contact tracing application is steadily, and significantly, increasing over time (p<.01), from less than 5% in week 1 to almost 25% in week 32[2]). By adding the data from Figure 4.3a on top of the participants who already have a contact tracing app, we find that approximately 68% of our participants have either already downloaded a contact tracing application or would be willing to download one under certain circumstances (including "an app that protects your data perfectly").

Estimates vary on how much of a population needs to participate in contact tracing in order for it to halt the pandemic, but recent work suggests a rate of around 60% [80, 87] to 70% [134], though [87] shows that automated contact tracing at any rate will slow the pandemic.

Our data show that even in the best possible privacy situation, with "an app that protects your data perfectly" (Q50), many participants have reservations about using an app to study or mitigate COVID-19. Results from other surveys about the same topic have shown a willingness to download ranging from 27 to 84%, depending on the population and exact situations presented. The wide range of willingnesses in related work suggests that further

[2] Some participants may have misunderstood the question asking whether they had a contact tracing application and answered 'Yes' when they did not have an app. In a cursory estimate, we find that about 10-15% of participants wrote mainstream apps like "Google maps" instead of a contact tracing app; however, here, we count *all* 'yes' answers because it is possible that the participants who answered incorrectly *believe* that they have a contact tracing app, given that the incorrect apps are still likely to ask for location or Bluetooth permissions.

work is necessary to examine the differences between the populations studied and the exact situations presented.

4.5.2.4 From participants' perspectives, location tracking presents privacy and security concerns that proximity does not; participants also reasoned about equity and technical accuracy

Participants did not exhibit a strong preference for proximity tracking over two other forms of location tracking in our quantitative data (Figure 4.3), potentially due to bias inherent with question ordering since location tracking situations were presented first. However, qualitative data reveals underlying privacy concerns about location tracking compared to proximity tracking, as well as concerns about privacy and efficacy of proximity tracking itself. We also find that inaccurate mental models of technology and contact tracing drive individuals' concerns, values, and willingness to download.

Participants have technical security concerns with proximity tracking. Proximity tracking evoked security concerns, with participants specifically concerned about anonymity and the security risks of their phone communicating directly with others': "*I don't want the phones to be sharing information between them because it could be easy for a hacker to violate multiple phones privacy*" (W6P74). W16P59 imagined a scenario in which tracing close contacts instead of location might put political dissidents at risk: "*Again, there are MANY people for whom this would simply not be safe if our current government had that information. Identify, say, one person at a protest. Get the info of EVERY phone that came within 6 feet of them on that day, or in that timeframe, and suddenly a LOT of people are at risk that had not been identified, and most often had done nothing wrong.*" Though these scenarios raise questions about the accuracy of participants' mental models of proximity tracking, they reveal that participants' concerns about the technical safety of a contact tracing method drive their willingness to enroll in automated contact tracing initiatives. Additionally, recent work has shown that many contact tracing apps have suboptimal privacy and security properties [265, 289, 319], so even if participant' mental models were inaccurate, their fears were not unfounded.

Qualitative data shows fewer privacy concerns with proximity tracking than with location tracking. Despite their concerns about privacy, 98 participants wrote a response that indicated they preferred proximity tracking, while only 13 preferred location. 18 indicated that it depended on who ran the service. Those who preferred proximity tracking considered it less invasive than location tracking. W9P100 brought up concerns about contact tracing data being shared with both companies and their government, and reasoned that proximity data better preserved their privacy: "*Proximity will probably be easier to swallow than location. There's something fundamentally unsettling about companies / my government having a record of everywhere I've gone, for how long I stayed there, etc. Knowing who I've passed on the street or purchased a burrito from, but not precisely where I passed them or exactly when I bought the burrito would be much less uncomfortable.*"

Participants reasoned about accuracy and effectiveness of both location tracking and proximity tracking. This reasoning revealed inaccurate mental models, e.g., "*I think that proximity tracking is more effective...as it would... be able to alert others and possibly stop them further spreading it, whereas location tracking would only really give an insight into where the virus is spreading*" (W6P23). Taking the opposite stance, W9P46 wrote: "*This method [proximity] appears to be better in a user data protection sense. But it does not provide the same benefits to the government that location data would. Location data enables lockdown and focus on specific areas with recent outbreaks.*" Other participants were concerned about proximity tracking not capturing surface transmission: "*There is also some evidence about catching from surfaces that others have touched, so location tracking may also be relevant*" (W14P67). Regardless of the accuracy of participants' mental models—both about the mechanics of automated contact tracing and about virus transmission—their concerns about efficacy reveal that they value a technology that they believe can *accurately* conduct automated contact tracing, and that their views of what technology is most likely to produce accurate contact tracing results will play into their decision to download.

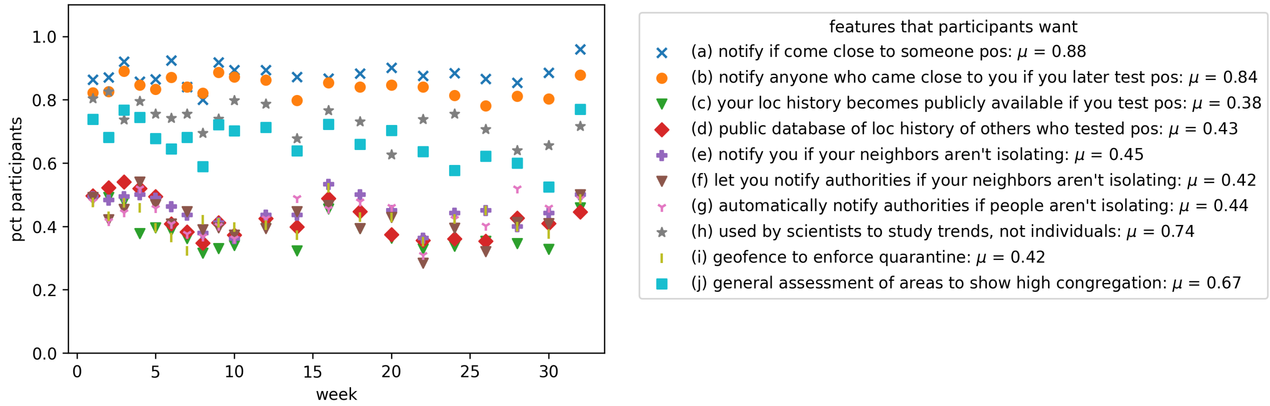


Figure 4.4: Features desired by participants in a COVID-19 tracking app (Q72).

4.5.2.5 Participants desire bare-bones contact tracing and informational features, not an app that might enforce quarantine or reveal personal information

The features or functionality of an app may also influence how many people are willing to download it. Participants responded positively to four of the ten potential app features[3], shown in Figure 4.4: they desire contact tracing notifications (a, b) (μ = 88%, 84%) and general reports on trends (h, j) (μ = 74%, 67%). All other potential features received less than 50% support.

In qualitative responses (Q74), 106 participants indicated support for informational features, with 44 desiring general information such as news and safety guidelines, and 62 expressing interest in location-specific resources such as information about nearby hospitals. W6P97 suggested that "*it would be useful to have a hotline or chat where you could be evaluated and diagnosed,*" and W1P54 thought it would be useful for a contact tracing app to "*provide national announcements and guidelines so that people get them in a clear, uniform fashion.*" 31 participants also expanded upon (j), expressing support for an app that shows COVID-19 hotspots, and 39 supported the options to notify (or be notified) if in contact with a positive case (a, b). Participants' desire for an *informative* app raises the question of

[3] All features were drawn from existing or proposed designs as of April 1, 2020.

whether access to reliable information about COVID-19 is an issue.

Concerns about security, privacy, equity, and access also arose. 41 participants mentioned anonymity, specifically bringing up stalking, harassment, and other forms of app abuse. Participants also reiterated their desire for health information to be shared with scientists, health professionals, and family, but not with the public. Though 16 participants wanted enforcement of rules to keep themselves or others safe, others were strongly opposed to this idea, citing concerns about fairness: "*I would prefer it to only inform and not gather any data or contact any law enforcers because everyone has their own circumstances and there might be people who cannot be on quarantine because of being not wealthy enough.*" (W6P53). W14P75 noted that developers must be mindful of resource consumption and backwards compatibility lest they risk excluding people since "*not all of us have the privilege of having the latest models.*"

4.5.3 App developer identity matters: (Mis)trust in government and some companies

We next more deeply investigate the privacy concerns revealed in Section **??** by exploring participants' trust in both government agencies and well-known tech companies. We find that:

- **Participants trust companies they perceive to be competent and resource-rich** (Section 4.5.3.1). In both qualitative and quantitative responses, participants indicated trust for Google over other companies.

- When weighing pros and cons of generic entities (e.g., government, university researchers) that might create a contact tracing app, participants go through a **complex decision process**, with no entity preferred by all and both positives and negatives about each of the entities we presented (Section 4.5.3.2).

- Participants conveyed substantial **mistrust in their government** (as a generic entity) conducting contact tracing, but displayed more trust in government health agencies and,

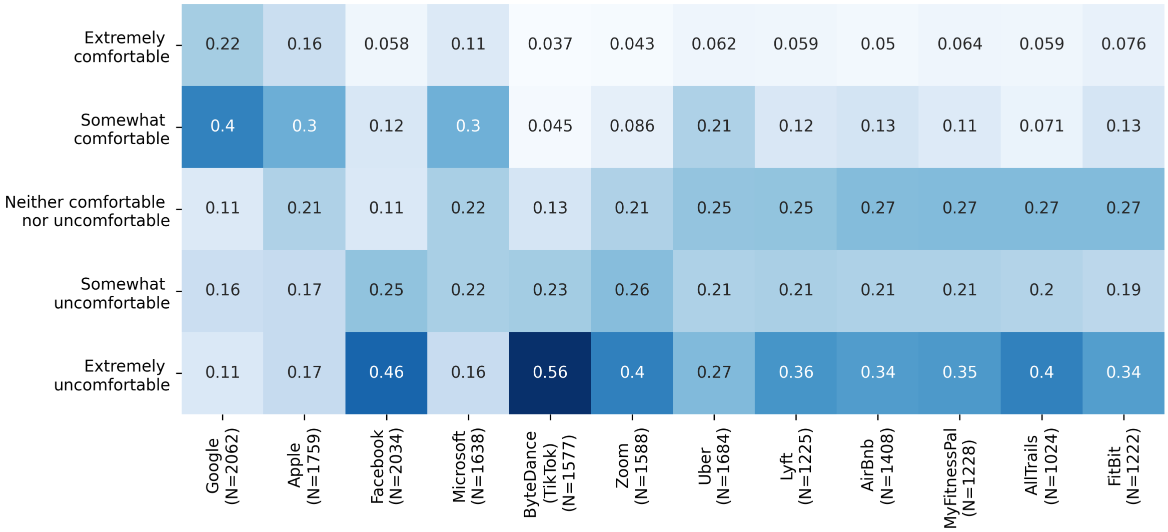


Figure 4.5: Participant comfort with a known company creating a *new* app using their location to study or mitigate COVID-19 (Q56). Due to longitudinal stability of the data, we combine all data here in order to show nuances in opinion. Columns sum to one and represent only participants who responded to the question and did not choose the option "I do not know enough about this company to make a decision."

in some circumstances, judicial oversight of government (Section 4.5.3.3).

4.5.3.1 Participants prefer large, known, already-trusted tech companies over other tech companies

Our survey asked both about a known company adding contract tracing to an *existing* app vs creating a *new* app to trace contacts. Though these situations require subtly different threat modeling, the results were similar; here, we present numbers from the question about a *new* app since that more closely reflects today's reality.

Participants indicated trust in large tech companies that have a good reputation concerning security and privacy and that they perceive to be capable of conducting contact tracing. More participants indicated comfort with Google or Google products than with any other company (μ = 62% comfortable), as shown in Figure 4.5. Participants also indicated some comfort with Microsoft and Apple (μ = 41 % and 46% comfortable, respectively), as shown in Figure 4.5. Less than 30% of participants indicated comfort with all other companies. Participants displayed the least comfort with ByteDance (TikTok) (μ = 79% uncomfortable) and Facebook (μ = 71% uncomfortable).

Qualitative analysis results reveals themes around user values and concerns regarding what apps they would trust most (Q23) and least (Q24) to use their location data for COVID-19 tracking. In line with the quantitative results reported above, 1205 users picked Google Maps or another Google app as their most trusted app and 431 picked Facebook as their least trusted app in the context of using location data for COVID-19 tracking. Reasons for picking their most trusted app, or for not picking their least trusted app, include the following:

Pre-existing technical capabilities, user base, and resources. Participants value a company that already has a large user base, sufficient monetary resources to add contact tracing to its capabilities, and the technical resources to implement accurate contact tracing (from participants' perspectives). W2P60 wrote: "*I would trust Google maps because it shows the most accurate current location real-time. I believe Google maps has the resources and manpower to allocate where I've been and when, I trust a more accurate and informational app. I imagine an app such as Instagram would be inaccurate because anyone can pick a location when they post a picture.*"

Some participants preferred an app in which location tracking is already central to its purposes (e.g., Google Maps, fitness apps, Uber, Snapchat, Pokemon Go), which they believed was a sign of technical capability to conduct contact tracing via location tracking. W8P77 explained, "*I would trust Google Maps or Apple Maps the most. Mainly because the app is made to track your location. Other apps for things like social media don't necessarily consider location as a huge factor of the app so I would feel more comfortable using an app that already tracks your location to determining spread of COVID-19.*" Others trusted a mapping app additionally because it was *not* social media and therefore maintained a degree of anonymity: *"Google Maps because it does get the location access, but not more of my personal data like instagram or facebook etc, where all my contacts and photos are"* (W2P151).

Already use and trust the app. Participants value an app that they already know and trust either because they feel like they understand the app's data sharing and privacy procedures or because they have already ceded privacy to that app: "*Waze, it uses my data anyway so why not*" (W1P125), and W3P3: "*I am ... locked in Apple's ecosystem, so they likely have all the data about me anyways.*" W4P17 clarified that it was less about trust and more about risk management: "*not necesarily trust, but resignation- I know Google and Waze already know my whereabouts and am resigned to them having my data.*"

Positive history and reputation with respect to security and privacy. Participants preferred a company known for protecting user data and making secure and private apps. W14P85 wrote: "*I would probably trust google maps the most since most of the other apps are known to be susceptible to data breaches/leaks in the past.*" W16P93 commented: "*I trust banking applications the most, because storing money is a serious matter,*" while W14P43 wrote that they trusted WhatsApp the most "*as I know it's encrypted and is very hard for mallicious hackers to break into to find my data.*" On the other hand, W1P75 wrote that they would not trust Facebook because "*Facebook is notorious for selling user data to third parties, and I would be very uncomfortable to know that they are tracking my location with the purpose of researching COVID-19.*" 14 participants wrote that they would not trust an app developed in China, e.g., TikTok: "*TikTok because I heard it sends user data to China*" (W2P140).

Participants also considered privacy policies: W5P91 preferred Apple because "*Apple have a reliable privacy policy and therefore I would trust this the most as I don't believe any of my data would become public without my permission.*"

Company-agnostic concerns about privacy and personal harm. Participants also mentioned concerns that extend to any contact tracing program and reflect broader themes throughout this survey: (a) stalking or personal harm due to poorly anonymized data, (b)

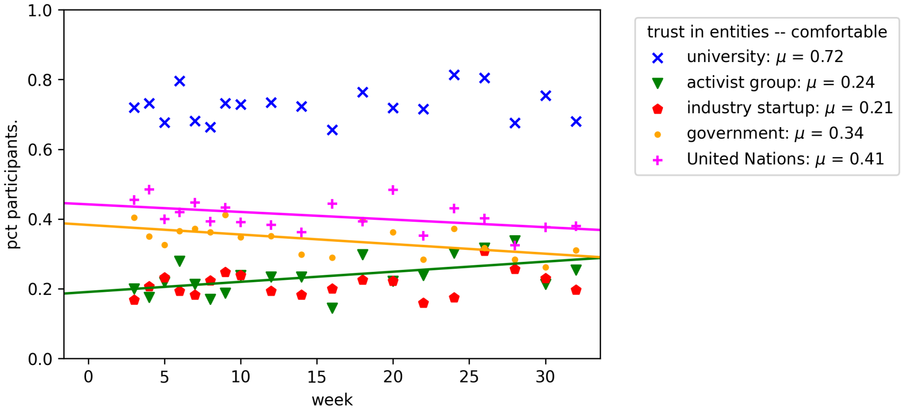


Figure 4.6: Participants' trust in generic entities (Q126). The higher reported trust in universities could be due to response or selection bias, as participants were shown the logo of our university before beginning the survey.

data leakage or privacy breaches, (c) data being sold by the company, and (d) a "slippery slope," in which this sort of tracking eventually becomes the norm.

4.5.3.2 Mixed trust levels for non-corporate generic entities

Stepping back, we asked for participants' comfort with *other* types of entities developing a contact tracing app. Participants indicated general mistrust for a potential new COVID-19-tracking app created by an industry startup (μ = 21% comfortable) or an activist group (μ = 24% comfortable), as shown in Figure 4.6, but were largely split on generic trust for a government- or United Nations-developed app. Responses indicate the most would place trust in a university-developed app (72% comfortable), but we note that at the beginning of the survey, participants were shown our university's logo and told that this survey was an academic endeavour, which may have caused response or selection bias [74]. In contrast, Hargattai and Redmiles found that universities would be one of the least trusted entities, at less than 10%, while a survey by the Washington Post and the University of Maryland found they were relatively trusted, at 57%. This discrepancy highlights the need for multiple surveys and qualitative data to better understand the nuances of public opinion.

Qualitative data revealed nuanced decisions around trust of a company or entity, echoing themes of general reputation and ability to both technically conduct contact tracing and protect data, while adding in participants' beliefs about the *intentions* of a given entity. As such, 86 wrote that they would trust an app developed by scientists, universities, or researchers over any other entity.

Participants argued both for and against the entities in Figure 4.6, revealing complex and individual decisions. Generally, participants indicated that trust depended on an entity's (a) intent to share or sell data, (b) anonymity or privacy guarantees, (c) reputation with respect to privacy and security, and (d) commitment to transparency and consent. Some expressed a desire for a regulatory body or for open source apps.

Some would support a tech startup because there is "*less notoriety attached to the brand*" (W9P55) and because they do not already have *other* data about the users; others would trust a big company because of its resources, credibility, and stability. Some participants considered activists unstable, unreliable, not credible, and incapable of actually securing data properly, while others valued activists groups' purer intentions, i.e., they believed that activists groups, unlike tech companies, would not sell the data on principle.

Participants who wrote about the UN mentioned its power and resources, but its international status was a plus for some (due to mistrust of their own government and not believing the UN would sell their data) and a minus for others (who disagreed with past UN work or believed the UN would be unable to produce a solution that worked for every country). W6P74 wrote in favor of the UN: "*If an International Organization such as the United Nations built the app and manages it, I will be more comfortable using the app because is a superior force than a government whom can use my data for electoral purposes or a company whom can use my data for profit.*"

Participants also raised several *positives* that they would expect from a government-developed app compared to other entities: governments cannot profit off the data, can keep companies in check through policy, and have a degree of legitimacy. W8P50 wrote in support of technical and regulatory transparency: "*I would feel most comfortable if the app was open sourced for the public to be able to scrutinize, by a government agency to remove any profit motivation to misuse the data, and would feel most comfortable if the data was stored in aggregate rather than individual tracking (no data as to where I personally am at a certain time, but rather on a population level what % are at home, near other app users, etc).*"

4.5.3.3 Trust in government health agencies; mistrust for "the government" as a whole, with strong concerns about proper data use and sharing

We find that participants are more comfortable sharing location or proximity data with governmental health agencies (as opposed to other sectors of government), and that more participants are comfortable with their location or proximity data being shared with their government only if they test positive for COVID-19, echoing trends from Section 4.5.2 and reemphasizing the need to protect the privacy of those who test positive. We find no strong regional trends concerning trust in government, as noted in Section 4.5.5, but other surveys have addressed this question more thoroughly, e.g., [20, 102, 171].

Participants indicated significantly higher comfort with their data being shared with health agencies for contact tracing (in line with previous work [243]), as shown in Figure 4.7 than with other government agencies. More participants were comfortable with both federal and local health departments ($\mu = 57\%$ federal; $\mu = 63\%$ local). Many fewer participants were comfortable with other agencies, i.e., local law enforcement ($\mu = 20\%$), immigration authorities ($\mu = 14\%$), and a tax agency ($\mu = 7.3\%$).

Concerns about data overuse and data sharing. Participants indicated substantial concerns about their government's use of data and about non-consensual data sharing with or within their government. 65 participants believed that the benefits of sharing location or proximity data with their government, especially with local or national health departments, would outweigh any negatives. Of those, 39 imagined restrictions on governmental data use and retention, such as that their government should delete the data after the pandemic. 36 wrote that sharing should be voluntary, and 27 said the US government should not

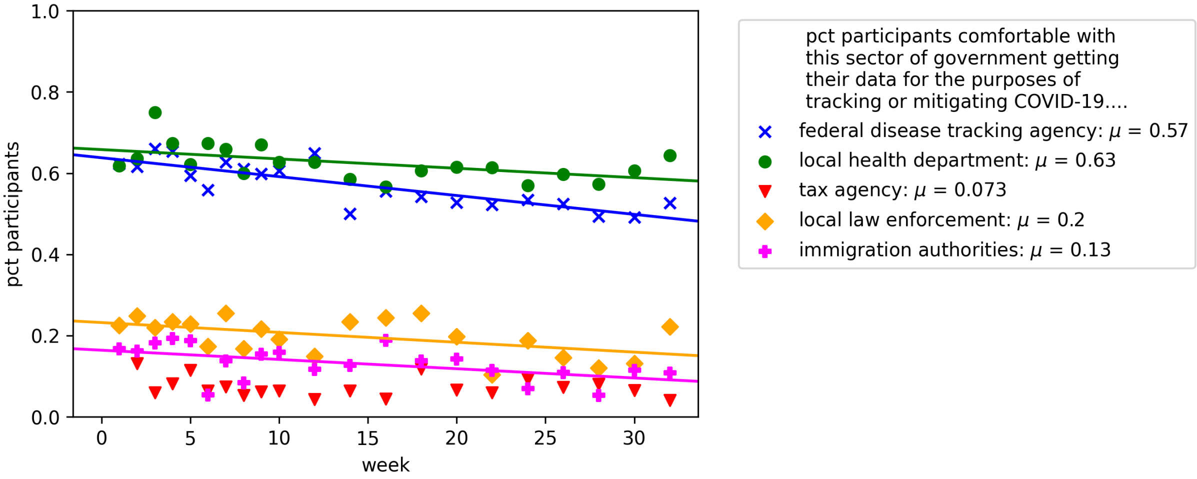


Figure 4.7: Participants' comfort with specific government agencies receiving their location or proximity data for the purposes of contact tracing (Q69).

share the data with Immigration and Customs Enforcement (ICE). However, quantitative data indicates a lack of trust that their government would use its citizens' location data conservatively: 72% responded that it was unlikely that their government would delete the data (Q66), and 69% said it was unlikely that their government would use it only for COVID-19 tracking (Q67).

Participants also indicated concern that such data sharing or collection would be harmful to their safety or the safety of those in their community (Q68), with 65% responding that they were extremely or somewhat concerned. W6P58 wrote: "*There is no chance they're going to only use it for Covid, especially in the states, and it could be very dangerous for many people, especially marginalized groups.*"

Mixed trust for judicial oversight of data sharing and use. We observe a clear preference for judicial supervision if data is shared from users regardless of health status, and no preference if data is shared only from COVID-19 positive users, as shown in Figure 4.8. We also observe that participants' perceptions of judicial oversight is grounded in their mental model of their judicial system and government; thus, overestimations of the level of

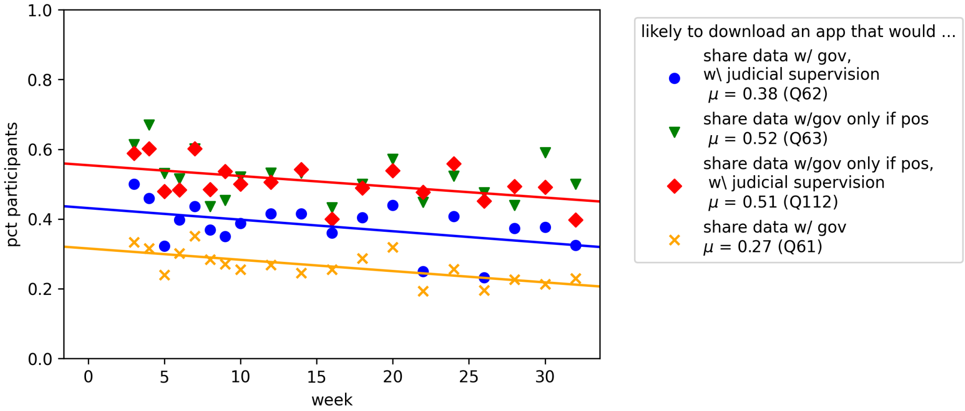


Figure 4.8: Participants' self-reported likelihood to download an app that shares their location data with their government under various conditions – sharing only when positive and with judicial supervision of the government's use of data. This plot shows only those who have *not* already downloaded a contact tracing app (unlike Figure 4.3).

corruption or self interest in the judiciary could skew trust and affect decision making.

Despite this preference for judicial supervision, and the increase in willingness to share if positive, 220 participants were overwhelmingly negative about judicial supervision in qualitative data, citing general concerns about not trusting their government, concerns about data sharing or usage for another purpose (142), as well as concerns about judicial impartiality (17) and tech literacy of judges (7). W30P50 (UK) wrote: "*No, judges can often be influenced by and working in a corrupt way with the government,*" and W28P76 (Poland) brought up bias and harm that could be introduced or exacerbated: "*I'm a member of a minority that our government doesn't like at this moment. I am extremely wary.*" Other participants felt negatively because they did not believe the judges would make the right decisions: "*The judges here in Canada suck, and can't be trusted to deal out justice properly. We have a revolving door justice system for criminals - what makes you think they'd do any better when things aren't as clear cut as criminal cases?*" (W22P88).

Participants commented on judges' digital literacy, citing that "*government officials,* *globally, seem to have a high rate of technology illiteracy*" (W14P83, Ireland). Instead, one participant suggested that there be "*data watchdogs and possibly even a human rights person*" (W18P98, Slovenia).

Some participants who were concerned about judicial impartiality actually desired oversight, but thought it would not be possible in their country due to corrupt or politically motivated judges: "*Would be more influenced if observed by an independent party not affiliated with the government or partners*" (W24P89, UK). W22P55 (US) wrote: "*Judicial oversight is a good starting point. But with the current administration, I feel like trust in the judicial system has been slowly getting eroded.*" Alluding to different levels of trust, understanding, and different political systems, W26P89 (Chile) wrote that"*Judges in my country are not really that much better than politicians....*"

Despite many concerns about corruption, politicization, and bias, some participants did present positive values, including already trusting the judicial system and/or their government (115) or judicial oversight being better than none (24). W28P11 (UK) felt that judicial oversight would prevent corruption, instead of enabling it; they wrote that judicial oversight "*should prevent abuse of power.*" W26P71 (Portugal) wrote: "*I think judicial oversight of apps should be more common.*" Additionally, themes of consent arose (27) along with the idea that such oversight is already occurring (21). Echoing themes from Section 4.5.2, 32 participants reiterated that their government should have access to their location data only if they actually tested positive for COVID-19.

This combination of qualitative and quantitative data tells a complex story about participants' trust in their governments, including trust in the legal system, as well as their understanding of how both judicial oversight and contact tracing operate. It also reflects the seemingly directly competing values of privacy and altruism that push people towards not sharing data and pull them towards sharing it for the common good. Again, participants' mental models of the mechanism in question here, the judicial system, may be inaccurate or incomplete, but still drive their willingness to participate in automated contact tracing. Additionally, political and judicial systems differ across the globe, and judicial oversight may be appropriate in some countries and not others.

4.5.4 Mixed attitudes about alternate data sources

We now review participants' opinions about data sources *other than* smartphone apps: cell tower location data, credit card history data, public sensors (including surveillance cameras), and electronic wearables. We find that:

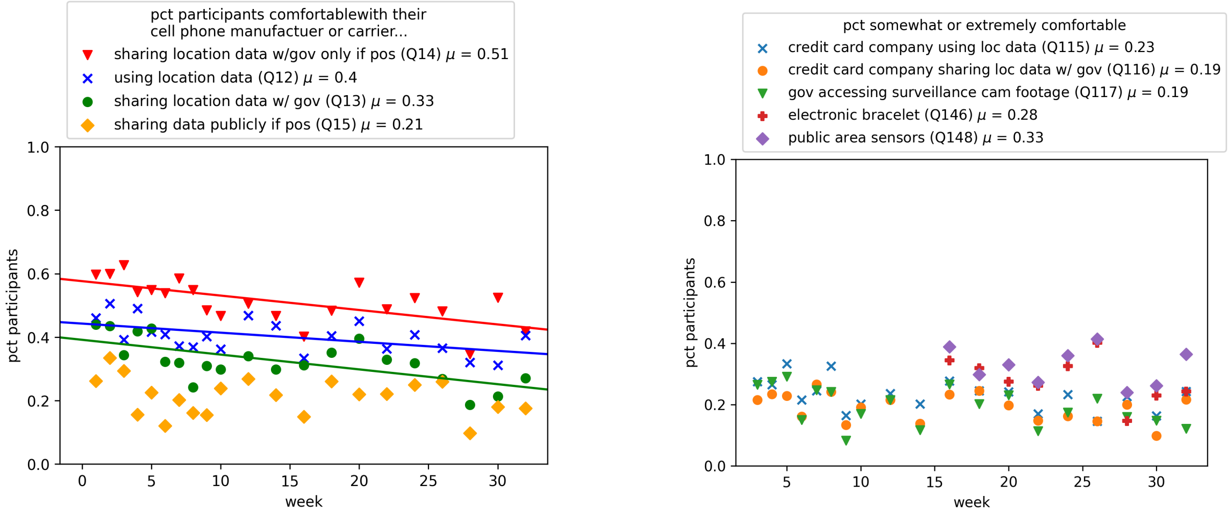
- There is **more support for contact tracing using cell tower location data than for the other non-app data sources** we asked about.

- Many of the concerns and values about smartphone contact tracing are magnified with non-smartphone automated contact tracing. Specifically, we observe that **consent for data collection, use, and sharing is extremely important to participants**, and particularly relevant to these non-smartphone data sources, which can largely occur without the user's informed consent. We call on the stakeholders in power to critically examine the need for consent beyond a terms of service agreement.

4.5.4.1 Support for cell tower data over other data sources

Regarding comfort with cell tower data being used for contact tracing, participants were most comfortable with their government being given the data if they tested positive, and many fewer were comfortable with the data being released publicly, as shown in Figure 4.9a. This preference resembles the increase comfort with data sharing *if positive* (Figures 4.8 and 4.3, Sections 4.5.2 and 4.5.3).

We observe statistically significant but slight downward slopes for three of the questions, and we note that the order of participants' comfort is largely consistent across weeks: the most participants were comfortable with their cell phone manufacturer or carrier sharing data with their government if they are positive ($\mu = 51\%$), and the fewest were comfortable with their location history being shared publicly if they tested positive ($\mu = 21\%$). This sentiment



(a) Attitudes towards cell tower location data being used for COVID-19 tracking: participants who said they were somewhat or extremely comfortable with their cell phone manufacturer or carrier using their location data for the purposes of COVID-19 tracking.

(b) Attitudes towards other data sources: participants who said they were somewhat or extremely comfortable with electronic wearables, public sensors, surveillance cameras, or credit card data being used for contact tracing.

Figure 4.9: Participants' attitudes about cell tower data and other data sources.

of being uncomfortable with public disclosure more generally underscores the importance of contact tracing data being properly protected when and if collected to avoid data exposure were a breach to occur.

As shown in Figure 4.9, participants were much less comfortable with their credit card history being used for contact tracing: $\mu = 23\%$ comfortable with contact tracing done by the credit card company, and $\mu = 19\%$ comfortable with that data going to their government. Participants were generally uncomfortable with their government using footage from surveillance cameras or other public area sensors for contact tracing ($\mu = 19\%$ comfortable with surveillance cameras and $\mu = 33\%$ comfortable with public area sensors) as well as with electronic bracelets ($\mu = 28\%$). We find no significant longitudinal trends.

4.5.4.2 Qualitative data reveals privacy concerns and the need for informed consent

Through the qualitative data, we find similar thematic concerns as from Section 4.5.3 about privacy, data sharing, surveillance, equity, accuracy. Participants also reiterate the need for meaningful consent and transparency. We emphasize, again, that there is no perfect data source, and that users will likely have privacy concerns about any potential source. As such, the technology and policy communities must assume responsibility for protecting and informing users about personal data acquisition and use.

Concerns about privacy, anonymity, and data sharing regarding alternate data sources. Privacy and anonymity were of paramount concern, especially with regard to public sensors and cell tower data, with many mentioning a "surveillance state." 88 participants wrote that the use of cell tower data for contact tracing could be a "slippery slope" towards more permanent privacy invasion or other misuse of data. 31 specifically referenced George Orwell's 1984 in reference to contact tracing data from surveillance cameras. W3P122 wrote: "*I'm very against expanding the surveillance state, even for a good reason, because it's never going to get rolled back.*" 67 participants were also uncomfortable with the idea of wearable electronics, with 22 specifically associating it with feeling like a "criminal," "prisoner," or "animal."

132 participants had concerns about the privacy of cell tower data, focused on the data being publicized or shared with their government (see Figure 4.9a); 68 of those specifically mentioned anonymity as a value. In responses about using credit card data, 53 specifically considered the sensitive nature of financial data. Some participants considered credit card data less private because it "*gives only a handful of specific locations, and not a complete timeline of every location like a phone would*" (W16P59), while others mentioned a mistrust of financial institutions ("*Credit card companies are not customer friendly and are always behind monetary benefits therefore I would not like them to have my data and trust them*" W3P20). These responses also suggest that participants' mental models of the privacy of

their credit card history is that location tracking would involve revealing their purchase history, which may be inaccurate.

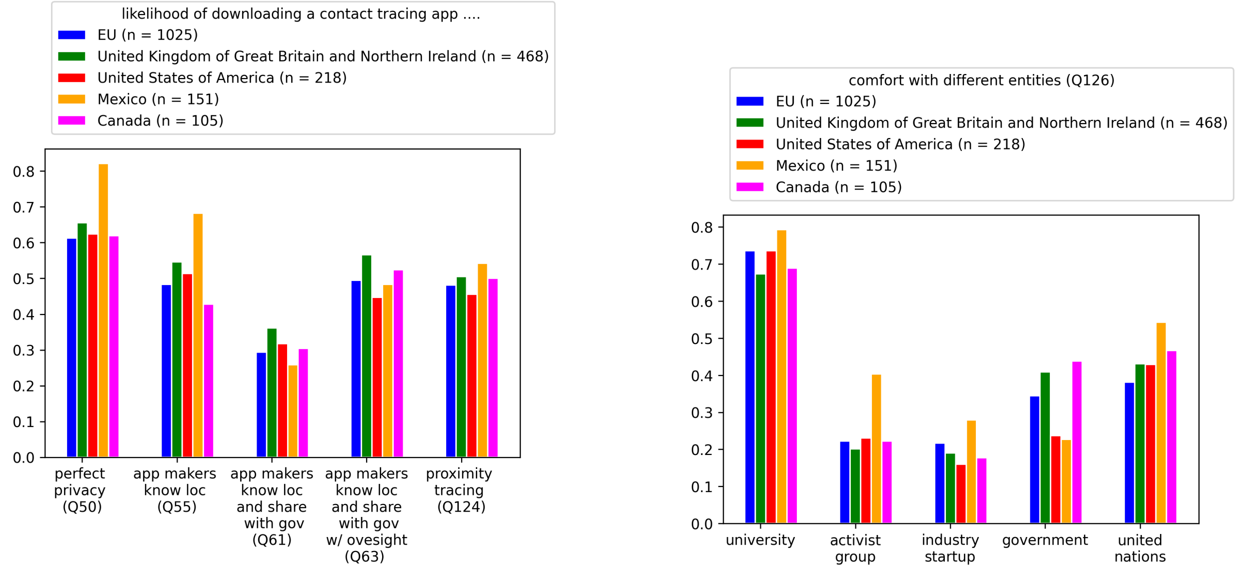
Concerns about equity, discrimination, and personal harm regarding alternate data sources. Participants raised concerns about the potential for discrimination, harm, and equity, echoing concerns from privacy experts [279] and emphasizing the need for technologists and policy makers to take extraordinary and thorough measures to protect potentially vulnerable populations. 17 participants feared harassment, prosecution, or discrimination with the use of cell tower data: "*if the location of people that has tested positive for COVID-19 is publicly shared, they might get targeted and hurt (or worse). This last idea comes from the fact that this was a situation given in my country, where it was publicly shared that a group of immigrants was tested positive, and this lead to them being persecuted*" (W16P98, Chile). Another participant mentioned the concern "*that people would would draw conclusions from (for example) two people being at the same hotel at the same time*" (W20P89). This situation is reminiscent of South Korea's initial handling of location tracking: location data and biographical details were posted publicly and were not sufficiently anonymized; groups discovered the identities of those who had tested positive and rumors started about extramarital affairs and plastic surgery trips [166]. South Korea has since started anonymizing the publicly released data more thoroughly [275].

Speaking to a theme of equity, some participants wrote that contact tracing using credit card data would be ineffective because "*credit cards are only for the elite*" (W3P33, South Africa). W3P63 extrapolated further, raising concerns about the potential societal implications of health information being linked to financial status: "*I fear this will lead to access to credit and my credit score being linked to my health or my compliance with social distancing. I am social distancing, but I worry about the future implications for this.*"

Participants also described the potential for harm caused through racial bias, specifically in reference to public sensors and surveillance cameras, recalling numerous issues with existing facial recognition systems. Others were concerned about the potential for future misuse: "*Police have already been caught illegally using face ID software, I certainly wouldn't trust* *them [using surveillance camera data for contact tracing]*" (W7P30).

Concerns about accuracy regarding alternate data sources. Echoing themes from Sections 4.5.2 and 4.5.3, participants reasoned about the accuracy of alternate data sources, concerned that cell tower data, credit card data, public sensors, and electronic wearables could not provide sufficient data for accurate contact tracing. 94 participants raised concerns about the lack of accuracy of credit card data: W9P60 noted that credit card data would an inappropriate source of contact tracing data because it is "*not good enough to track movement. Park/beach and many more places where I would not use card but be around people.*" Participants also reflected on the potential for facial identification from surveillance cameras to fail (e.g., if wearing masks or sunglasses) or to be impractical due to cost or lack of population density. Reflecting on practicality, W16P71 wrote: "*A tracking bracelet may get lost or people may forget to wear it when they leave the house. It wouldn't provide the most accurate data.*"

Participants value consent and transparency regarding alternate data sources. Throughout all questions, participants raised concerns about consent and transparency, which are particularly important with data that could be collected without their knowledge or with minimal consent (e.g., through a terms of service agreement), for example, via public sensors or data that already exists, like credit card data or cell phone tower data. W1P190 wrote that an end-date for cell tower data collection and use would make them feel more comfortable: "*If I were informed in advance of the initiative and there was a sunset date for the initiative, I'd be somewhat likely to allow it for the purpose of scientific research. Absent my explicit consent and for only a short period of time, however, I'd be extremely uncomfortable with it.*" Even W12P86, who was largely comfortable with the use of credit card data for contact tracing, gave the caveat that "explicit consent" was necessary: "*I feel more comfortable with my location being acquired (with my knowledge and consent) via this method as it makes me more relieved that I am not actively being tracked (or my location is not being tracked and traced to beach movement). The usage of my credit card history allows me windows of privacy which I would not want anyone interfering with.*" Thus, policy



(a) Likelihood of downloading a contact tracing app versus location (for the countries from which we had at least 100 participants total). (See Section 4.5.2.)

(b) Comfort with generic entities creating a contact tracing app (for the countries for which we had at least 100 participants). (See Section 4.5.3.2.)

Figure 4.10: These figures show two sets of questions broken down by regional responses.

makers and technologists must both work to protect and inform users.

Some support for non-smartphone data sources for contact tracing. Though a majority of participants raised concerns, some supported the alternative data sources we asked about. Of those who supported (or did not oppose) the idea of cell tower data being used for contact tracing, 123 mentioned altruism and the greater good of contact tracing, suggesting that many users, under the right circumstances, may decide that the greater good of their communities outweighs some personal privacy concerns. 24 said they would accept such data sharing if it were for research, while 20 would accept only if they tested positive for COVID-19; these opinions raise questions about these participants' mental models of contact tracing or whether they would consider such data sharing as a way to reduce their need to quarantine if positive.

4.5.5 Demographic trends

Given the lack of strong longitudinal trends in many of the questions, we examined demographic trends by combining data from *all* weeks. We find no trends for age, gender, or time spent outside home. We also observe no correlation with infection rate (see Figure 4.1). The following section presents trends that are largely present throughout all questions; we show the questions related to willingness to use a COVID-19 contact tracing app.

Few regional trends appear in our dataset, but related work investigates more thoroughly. When examining regional trends, we include only regions (e.g., the EU) or countries from which we had more than 100 participants: EU, UK, USA, Mexico, and Canada. We do not find regional trends between the EU, UK, USA and Canada. However, we find that participants from Mexico are less willing to share data with their government, but perhaps more willing to give up privacy if their government is not involved, as shown in Figure 4.10 (as compared to participants from the EU, UK, US, and Canada). Others have studied regional differences in attitudes towards contact tracing applications [13, 20, 171], and there is a growing body work about cultural or regional differences in privacy attitudes and definitions more generally (e.g., [129, 260]).

Concern (or lack of concern) about COVID-19 correlated to willingness to download a contact tracing app or give up privacy. Perhaps unsurprisingly, as shown in Figure 4.11, we find that extreme concern about COVID-19 is correlated with greater willingness to download a contact tracing app or surrender some personal privacy for the sake of contact tracing. However, we also find that extreme *unconcern* is correlated with the same willingness to download a contact tracing app or give up some privacy. One possible explanation is that those who are unconcerned are more accepting of risk in general and thus may be more willing to take actions that others view as potential violations of privacy.

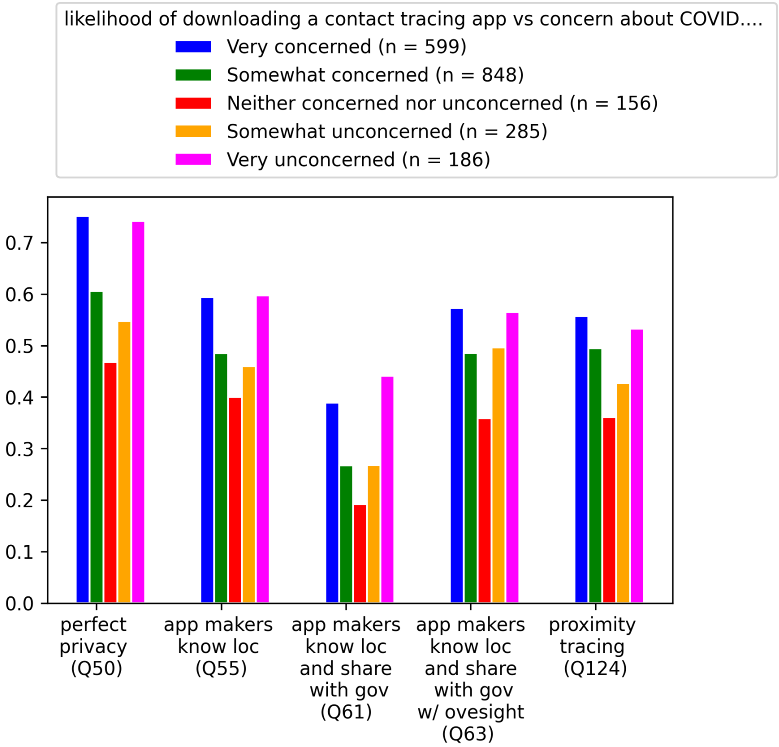


Figure 4.11: Willingness to download as compared to concern about COVID-19

4.6 Discussion

Drawing from our findings, we surface lessons for both researchers and stakeholders (including app makers, public health experts, policy makers, and others).

User education is needed to correct inaccurate mental models and therefore enable adoption. Users are concerned with the accuracy of the technology involved in contact tracing as well as companies' abilities to actually conduct contact tracing, but may be ill-equipped to accurately reason about these factors due to an understandable lack of technical training. Adding to recommendations by groups with similar findings [324, 330], we recommend that technology companies and governments conduct user education campaigns to teach users—at an appropriate technical level—to reason about the extent to which the contact tracing app available to them is appropriate for their personal situation.

Users value transparency and consent, and may be less concerned about privacy if they feel in control. Our data revealed substantial fears about data overuse and oversharing, echoing privacy concerns found by numerous others (see Section 4.3). Participants feared non-consensual data sharing with both their own government and foreign governments as well as data being used for purposes other than contact tracing (e.g., advertising, national security, etc). We recommend that policy makers continue to both create restrictive policies to make users comfortable and educate users about those policies.

An individual's willingness to download a contact tracing app depends on security and privacy *and other factors.* Beyond the privacy and security concerns and opinions that our work surfaces, there are many other broader issues that must be addressed with the release of a contact tracing application, some of which arose in our qualitative data: participants brought up concerns of accuracy, equity, and access to smartphones, as well as concerns about the harms of data overusage or sharing disproportionately affecting certain parts of the population. Building on those themes, we encourage stakeholders to consider *accessibility and usability by all*, including those who do not speak the majority language, those who cannot read or write, those who have one or more disabilities (e.g. vision impairment). Additionally, *not all people have smartphones*, and some high risk groups, such as seniors, may be less likely to regularly use a smartphone. A smartphone app excludes those sets of users. If a certain demographic group is left without access, or without usable access, they will benefit less from contact tracing, potentially resulting in different rates of infection. Thus, we urge stakeholders to explore acceptance for automated contact tracing in a broader context than strictly security and privacy and refer readers to [18, 120, 175, 236, 239, 279] for a fuller discussion of equity and efficacy concerns.

There are substantial challenges with future-proofing longitudinal work during a rapidly evolving global event due to changing terminology and technology. Terminology and technology have evolved *rapidly* during the COVID-19 pandemic, and we thus implore other researchers doing longitudinal work to carefully consider the phrasing of their survey. In designing our survey in late March, we knew we were trying to design questions that would remain relevant for months, throughout a rapidly changing world event. We designed our survey with a goal of being resilient to such world changes. We include our full survey in the appendix, and explicitly note when new questions were added, as the world and the global discussion around contact tracing evolved. Our key recommendations, to any future designers of surveys focused on rapidly evolving issues, are to: (1) design the initial survey with an eye toward future-resiliency, (2) strive to make sure that any additions or modifications to the survey do not invalidate longitudinal analyses, and (3) clearly document any such changes, so that the scientific community can fully evaluate the work and the results.

Researchers should continue to study acceptance for automated contact tracing within *specific* populations. Our survey focused on a longitudinal view of young, white, European and North American views towards automated contact tracing, but we were unable to study any one particular population in depth. Other work has studied populations at a single-country level, e.g., the Netherlands, Germany, Australia, but to our knowledge, few have focused yet on specific and potentially vulnerable subpopulations or minorities, who might have heightened or different privacy preferences, and who also might have greater vulnerability to the virus (one exception is Filer et al., who studied adoption and attitudes amongst health care workers in England's national health care system, the NHS [90]). We specifically call for further research on minority populations that may be harder hit by the virus (e.g., communities of color in the US [155]), communities that may have a more strained relationship with government or authorities (e.g. Black communities in the US, undocumented immigrants, political dissidents), or communities that may remember a past epidemic (e.g., gay men who lived through the AIDS epidemic). Despite certain communities being particularly vulnerable, we are not aware of existing studies about contact tracing and privacy for such populations, and we believe it is crucial for future work to study and address the specific contexts of these groups.

4.7 Conclusion

Here we have presented results from a longitudinal survey about public opinion surrounding location privacy and contact tracing during the COVID-19 pandemic, finding that public opinion is largely stable over time, and that they have significant and diverse privacy concerns about contact tracing.

This chapter adds to other work about public opinion on potential contact tracing technologies and privacy concerns, and we strongly encourage contact tracing developers, policy makers, and others to consider the user values and concerns presented here, as user cooperation is crucial.

Stepping back, this chapter has also explored themes about change and vulnerability in a global pandemic, specifically with regards to how security and privacy concerns can compete with other concerns, like health (theme 2). I have also shown how in the early days of the pandemic, people faced a lot of change and new technologies were introduced—contact tracing apps—leading to incomplete threat models about contact tracing apps (theme 1), and how they were particularly concerned about contact tracing apps and data being weaponized against marginalized groups (theme 3). Additionally, because Covid-19 has affected minoritized communities more severely [158], contact tracing apps that either cause more harm to these communities through computer security and privacy issues, or apps that go unused because of concerns of such issues, harm marginalized communities more.

Acknowledgements

We are very thankful to Karl Weintraub for general discussions, sanity, and his Pandas knowledge. We are also thankful to Gennie Gebhart for early discussions about this work. We thank Christine Chen, Ivan Evtimov, Joseph Jaeger, Shrirang Mare, Alison Simko, Robert Simko, and Eric Zeng for their valuable feedback on pilot versions of our survey. Additionally, we are thankful to Gennie Gebhart, Joseph Jaeger, and Elissa Redmiles for their valuable feedback on a draft of this paper.

We are also very thankful to Prolific for supporting our research by waiving their fees for one month as part of their COVID-19 fee waiver program.

This research was supported in part by a University of Washington Population Health Initiative's COVID-19 Rapid Response Grant and by the University of Washington Tech Policy Lab, which receives support from: the John D. and Catherine T. MacArthur Foundation, Microsoft, and the Pierre and Pamela Omidyar Fund at the Silicon Valley Community Foundation. This work was also supported by the US National Science Foundation (Awards 1565252 and 1513584).

Chapter 5

THE USE AND DISUSE OF TECHNOLOGY DURING HURRICANES

This chapter presents my work on technology use (and lack of use) during hurricanes. In this chapter, I study *access* to technology as one of the prerequisites for computer security and privacy, and explore hurricanes as a use case in which tensions arise between access to technology (due to damaged infrastructure) and information needs. I first overview how the themes about change and vulnerability appear in this chapter, and then present the research itself.

Change: a natural disaster. Hurricanes and other natural disasters occur regularly around the world, causing potentially massive damage to coastal communities. They cause **power, cellular, and internet outages, property damage, scarcity of basic resources like gasoline and food**, all of which may cause substantial **changes in one's daily routine**. Additionally, because hurricanes are natural disasters, technical security threat models may include opportunistic adversaries (e.g., scammers), but not adversaries directly responsible for each event.

Additionally, unlike some crises, hurricanes *are* predictable and regularly occurring; thus, preparation and mitigation are ongoing community and individual efforts.

Theme (1): a critical need for information during a time of constrained resources. During and after a natural disaster, people try to seek information about their community and connect with loved ones [115]. For example, weather information and information about community resources and safety may be rapidly changing and important for community members to receive completely and promptly. However, during and after a hurricane, communities often experience power, cellular, and internet outages due to **damaged infrastructure**, making use of many modern technological avenues of communication and information-gathering difficult.

Theme (2): prioritizing physical safety and critical information. In this newly resource-constrained environment, some have urgent physical safety concerns, e.g., property damage, medical emergencies, and evacuation from flood waters (for which they may need urgent help [332]). Once the storm has passed, the damage to the physical environment can still dominate everyday activities—for example, by limiting connectivity, power, access to food and potable water, and other basic necessities. We find that people do use technology when possible, but often decrease or limit use due to the constraints on resources, prioritizing current and future physical safety.

Theme (3): marginalized populations are hit harder by natural disasters and are therefore excluded from research on people who *can* use technology after a disaster. Much of the work on technology and disasters has focused on social media use during disasters, excluding those who are un*able* to access social media and other technologies. Because we found that lack of electricity of connectivity constrained individuals' technology use during and after a hurricane, in this chapter we urge future researchers to study the *barriers* to technology use. For example, apps that drain one's battery are ill-suited for low-resource environments and are an example of a design misalignment; however, we observe that marginalized and vulnerable communities are historically more severely affected by natural disasters due to lack of resilient infrastructure, poverty (affecting community resilience and preparedness), and inequitable distribution of information and resources in the recovery phase [91].

Co-authors. In this chapter, I use "we" to represent the work and writing done by my coauthors, Harshini Sri Ramulu, Tadayoshi Kohno, and Yasemin Acar. We began this work while I was an intern at the Max Planck Institute with Dr. Acar.

5.1 Introduction

Tropical cyclones, e.g., hurricanes, affect billions of people around the world, causing death and injury, physical damage to infrastructure, and billions of dollars in economic impact [215]. Personal technology, such as smartphones and home computers, can be a critical part of mitigating impact for affected communities. Indeed, during and after a disaster, people seek to secure their and others' physical safety, and then seek information about the disaster, their loved ones, and assistance [115, 273].

Prior work has explored how natural disasters can be a time of *technology adoption* and *innovation*. Indeed, communities come together on social media to exchange vital information about well-being and aid during the immediate aftermath of a disaster [48, 54, 201, 282, 314, 332], and researchers have studied or designed apps to be used specifically during crises both by individuals and by local governments or researchers seeking to track the disaster and the community in real time [287, 295, 331].

This prior work about technology innovation and adoption during crises is extraordinarily valuable because personal technology can indeed greatly help individuals and communities during and after a disaster [48, 54, 201, 282, 314, 332]. However, we observe two gaps in research about technology use during disasters, and through a set of qualitative surveys, provide a foundation for future research to address both, building upon recent work also inquiring about the over-prioritization of technology usage in disaster research [276]. We find the following two gaps:

Gap in prior work: holistic technology use during natural disasters. In order to best allocate resources, design technology, and implement policy, it is critical to have a *complete* view of technology use and non-use during crises. While there is a plethora of work on social media usage and the usage and design of made-for-crisis apps [295], there is little work about how other kinds of technology and information sources are used during crises. While the utility of social media is well documented, we lack a rich understanding of how other technologies and information sources—for example, weather apps, news sources, and communication tools—are adopted and used (or not used) during crises, and how these technologies respond to the underlying needs driving technology use during crises. While these types of technologies may not be designed with the same potential for crowdsourcing information and public study, they may fill other needs for users, and understanding why users choose to use or not use certain apps, or categories of apps, as well as how use of these technologies complement social media, can help direct future research, technology design, and policy proposals.

Gap in prior work: decreased or stopped technology use during natural disasters. During natural disasters, public infrastructure is often damaged, and access to electricity, internet, and cellular service may be decreased or completely lost for many. For example, after 2021's Category 4 Hurricane Ida, more than one million people in Louisiana were without power [1]. Decreased or lost access to utilities may affect what technologies people choose to use and whether they can use them at all. However, existing work focuses on those who *can and do* use technology—Twitter, Facebook, etc [247, 273]—and misses the *many, many* people who lack unfettered access to electricity, internet, and cellular connectivity after a natural disaster. Utility outages and utility restoration are also not distributed equitably [91], and, thus, a research community that does not study the effect of these barriers to technology use misses an opportunity to address systemic inequity.

To address these gaps, we conducted a broad qualitative survey with 138 participants from areas in the mainland US that regularly experience hurricanes and tropical storms. We choose to study just one type of natural disaster—tropical cyclones, the meteorological term covering hurricanes, tropical storms, typhoons, etc [211]—because different natural disasters differ in terms of predictability, preparation, short term experience, and long term recovery. 99 of the participants were simply living in hurricane-prone areas, recalling their experiences of past hurricanes; in order to complement that historical data, we also recruited 39 participants who were either experiencing a hurricane currently or who had just experienced a hurricane. Our IRB-approved surveys explored the following research questions:

- **(RQ1)** What do people experience during a storm? What **needs and circumstances** during a hurricane drive technology adoption, use, and disuse?

- **(RQ2)** Holistically, what does technology use look like during a hurricane, and in what ways does that usage represent a **change** (increase, decrease, adoption, disuse) from users' typical technology use?

- **(RQ3)** How do people respond, technologically, to the circumstances created by **physical infrastructure damage**, e.g., loss of power and loss of connectivity? What coping strategies do they develop, or what risks or costs do they take on by not using technology?

We find that there is substantial personal technology use outside oft-studied social media, and that people may adopt *new* sources of information and technologies during hurricanes, such as new weather apps and new local news source. However, we also find that decreased or severed access to electricity, internet, and cellular service drives individuals to decrease or stop use of some technologies, and that users prioritize technology use based on their needs, the perceived utility of the app, and the resource consumption of the app, leading them to deprioritize apps for which the utility is outweighed by the app's battery, data, and time consumption.

At a high level, these findings provide a *holistic* view of individuals' technology use during hurricanes, as well as the barriers to usage. From these results, we make recommendations for future research and technical design to support technology use in the low-resource contexts so often created by natural disasters, e.g., network design, system design, and security and privacy considerations. Our recommendations and results have broad implications and we believe that *many* research, technical, and policy communities can, both independently and together, address the problems that cause technology to be inaccessible or unusable during crises. Prior work has shown that technology can be a powerful tool in disaster recovery, so users should be *able* to use technology if they choose to, which means they must have the resources to use that technology and the technology must be usable, safe, and functionally important to them. We make recommendations at the level of network design and implementation, infrastructure policy, software design, and security and privacy research.

The rest of the chapter is organized as follows: we first overview related works in Section 5.2, briefly covering the vast amount of prior work in crisis informatics that explores technology use during crisis and technology developed for crisis, as well as harms amplified by crises. We then explain our survey methodology in Section 5.3, including recruitment, the modular nature of our surveys, and our ethical and safety considerations, especially when surveying people *during* a hurricane. We then turn to our results, exploring technology use and disuse in hurricane preparation, needs and circumstances driving technology use during hurricanes, changes in technology use during hurricanes, and coping strategies for lost access to electricity and connectivity. Finally, in Section 5.5 we conclude with a discussion of how various research, technology, and policy communities can move forward with research that helps communities that experience hurricanes.

5.2 Related Works

In this section, we explore prior work on technology use during natural disasters. We begin by overviewing research about technology use during hurricanes first generally, and then specifically on social media use during hurricanes, which is more numerous. We then touch on work about technology use during *other* disasters as well as technologies made specifically for use by the public during disasters (made-for-crisis apps). Finally, we briefly touch on interdisciplinary work about how systemic inequities further harm marginalized populations during natural disasters. We recommend Simon et al.'s 2015 survey or Reuter and Kaufhold's review of social media in crises for a more thorough literature review of the area [247, 273].

Social media used during hurricanes The bulk of the research on technology use during hurricanes has focused on use of social media, specifically, Twitter. According to the Pew Research Center and Twitter itself, use of Twitter increased dramatically during 2012's

Hurricane Sandy, with 20 million tweets sent about the storm in four days [125]. Of those 20 million tweets, Pew found that about a third were about news and information, a quarter were photos and videos, and the rest were jokes, hopes and prayers, political commentary, and excitement [125]. Indeed, other groups have explored increased use of social media during Sandy and other hurricanes, both generally [142, 170, 204] and for finding emergency aid [201, 332] and longer term disaster relief [204]. Kogan et al, for example, found that local ("geographically vulnerable") Twitter users increased tweet volume during Hurricane Sandy in 2012, and the information they tweeted or retweeted was "more likely to have some kind of local utility" [170].

Yang et al found that during 2017's Hurricane Harvey in Houston, TX, local governments, emergency services, and local news agencies were highly influential and active on Twitter, and, also, that Twitter users turned to Twitter for emergency help when 911 was overloaded or not working [328]. Others have also documented how people turn to social media for urgent help during hurricanes, e.g., Twitter users who requested boat rescues via tweets during Hurricane Harvey [201, 332].

Others have analyzed how local officials have used social media during hurricanes, finding that officials' messages vary in engagement, purpose, and effectiveness [98, 141, 182, 186, 328]. Hughes, for example, analyzed online communication from official local sources during Hurricane Sandy, finding that few local fire and police departments actively disseminated information or responded to the public on social media, but those that did showed compassion by responding to emergencies rather than directing all emergencies to 911, as policy technically required them to do [141]. In analysis of three major 2017 hurricanes (Harvey, Irma, Maria), Li et al. found that during the storms, official accounts, which are tagged in far more tweets than they respond to, responded more frequently to tweets that were on-topic (e.g., about the hurricane or about power outages) and provided insight rather than political commentary or informalness [182].

Our work diverges from this body of work and explores the less-studied *non-use* and *decreased usage* of technology, in addition to adoption and changed usage of technology and

Twitter, as explored in these works. While social media is a critical tool in crises, and can democratize dissemination of important information, it is also important to focus on the *barriers* to use and *disuse* of social media and other technologies, as well as how people use social media in the context of other needs and technologies.

Overall technology use during hurricanes In addition to the works above about about social media use during hurricanes, there have been a few more broadly about technology use or disuse during hurricanes, which we overview here. One relatively early paper, by Shklovski et al., is particularly relevant as it explores the adoption of technology use amongst the musician community in New Orleans after Hurricane Katrina (in 2005) [268]. Shklovski et al. found that mobile phones were a critical resource for not only the individual but for everyone around them and documented how musicians adopted new patterns of use in response to changing information needs and a resource-constrained environment—for example, many of their participants used SMS texts for the first time after Hurricane Katrina, as they required less connectivity and less power. Our data reveals similar themes of technology adoption because of loss of electricity and connection, but we note a significant difference, perhaps due to the differing technical contexts of 2021 and 2005 (Hurricane Katrina): Schklovski's participants found SMS, a new technology for some, largely sufficient for their needs, perhaps because they had other non-technical strategies for communicating and gathering information, or because they had different needs, or because the cellular network was operable enough for their needs, where our participants reported rationing technology use in response to resource constraints.

Ferris et al. surveyed New Jersey residents who evacuated after 2012's Hurricane Sandy, asking about the role of technology (social media, text messaging, phone calls, news media) in their decision to evacuate. They found that technology was used for "hurricane preparation, planning and evacuation," but that most technology use decreased after a hurricane (except text messaging), likely due to restricted access to electricity, cellular service, and internet [88]. Schwartz also studied the response to Hurricane Sandy, finding that those who lost access to technology felt both increased mindfulness and groundedness and increased powerlessness, boredom, frustration, and anger at the lack of control and lack of information and connectedness [263]. Der-Martirosian et al specifically study telehealth adoption by veterans during the weeks surrounding 2017's Hurricane Harvey, finding that telehealth use increased for users who were older or more medically vulnerable [77].

Though our work does not specifically bring up themes of mindfulness without technology, our results do also reveals both the criticality of technology and decreased usage in many cases, and we build upon this important work by (a) providing an *updated, 2021* view of technology use during hurricanes, (b) examining the use of technology more broadly during a hurricane, and (c) exploring, qualitatively, *why* people used technology the way they did.

Social media use during other crises. Social media use during crises extends beyond hurricanes, as many in the crisis informatics community have explored [223]. Many have explored the increased in social media use during specific crises, including during wildfires [314], flooding [48, 314], terrorist attacks [216], earthquakes [180, 259, 277], and the Covid-19 pandemic [278]. Some include the effect of destroyed infrastructure in their analysis, including Li et al., who wrote that Twitter's short text-based nature meant that it was one of the few technologies people could adopt when cellular and power infrastructure was destroyed during the 2008 earthquake in Sichuan, China [180].

Work has also specifically focused on the geographically distributed online communities of digital volunteers that help those seeking information during a disaster with reliable resources [54, 278, 282]. Others have focused on social media use by emergency management or local government as a means to distribute critical information and monitor the community in real time via public information, finding broadly that use of social media by local officials varies widely but can be both effective in dispersing aid *to* the community and in gathering information *about* the community [176].

Additionally, researchers have focused on mis- and disinformation during crises and the role of communities in supporting or correcting rumors, e.g., during Hurricane Sandy [124], Hurricane Irene [68], and the Boston Marathon bombing [281]. Gupta et al analyzed 10,000 fake image tweets during 2012's Hurricane Sandy, finding that there were few original images and that only a few people were responsible for most retweets [124]. Lovari et al. found that local officials are concerned about spreading misinformation on social media and they are understaffed [186]. Endsley et al. found that people trust information from news media (both local and national) more, but that social ties also influence trust (e.g., who the info is from) [82].

Crisis apps. There is also a growing body of work on apps that are specifically made for use during crisis; our work builds on this work by gathering data about real-world use of these apps. In a 2017 literature review, Tan et al analyzed 49 papers about crisis apps, 35 of which were apps built specifically for disaster (e.g., "Hurricane Hound"), and others of which were general purpose apps that people use additionally during a disaster (e.g., Facebook, Twitter, Google). Tan et al. focused on the 35 built-for-disaster apps and categorized them by *purpose* (e.g., crowdsourcing information, information dissemination) and *contribution* (preparedness, harm mitigation, response, and recovery) [295]. Tan et al. identified user perceptions of crisis apps as a gap in literature [295]. Since their 2017 literature review, Appleby et al. found, with Italian and German participants, that crisis apps increased users' trust in local institutions (emergency services, police, news media) by creating a sense of shared responsibility during a crisis, and that users perceived made-for-disaster apps as more reliable than general purpose social media apps specifically during disasters [25]. In a 2020 study, Tan et al. conducted a mixed-methods study about what makes users *keep* crisis apps, finding that utility and dependability were key, but making no mention of security, privacy, or trust as a factor in their paper or their interview or survey materials [294]. Multiple groups have studied older adults' perceptions and use of crisis apps [287, 331]. Zhang et al. study how older adults used crisis apps during a natural gas explosion in Pennsylvania, finding that, in general, engagement with the apps was low, but that community involvement was critical to app adoption for those who did use them. They also found that older adults may not trust crisis apps, citing concerns about misinformation, scams, and general mistrust of certain platforms [331].

Systemic inequity during crises Recently, some work within the HCI community has explored how technology can increase, or create inequity during disasters. Soden et al. argue that the disaster technology and informatics created gaps and “silences” during the aftermath of the 2015 Nepal earthquake that “foreclosed opportunities to address important challenges that the people of Langtang faced” [277]. Madianou explores how the digital divide amplified existing social inequities during 2013’s Typhoon Haiyan in the Phillipines, leading those who used social media and smartphones to get recover more quickly economically, and leaving those who did not have access to technology or connectivity to “languish behind” directly due to the lack of connectivity [190]. More broadly, it has been well documented that natural disaster response reflects and can deepen systemic inequities, e.g., access to assistance provided only in English in the US, or in places easily accessibly by public transit [91], infrastructure and housing being less sturdy in poorer neighborhoods [190], or researchers being accountable to donors rather than the communities they are studying [191].

Proposed systemic solutions specific to the research community and methodology remain rare. Soden et al present a highly interdisciplinary workshop on flood data as a methodological contribution towards bringing together experts from different communities and bridging the gap between technical disaster research communities and social scientists, artists, and local communities [276]. Gaillard et al. propose a disaster researchers’ code of conduct that urges researchers to reflect on who is benefiting from their work and amplify the work of locals [100, 101]. Such high level reflection on the purpose and direction of disaster research and crisis informatics remains rare in published academic work.

We add to this critical body of work by providing another view of technology disuse, as well as suggestions for a wide variety of researchers, policy-makers, and technologists.

5.3 Methodology and Background

In this study, our goal was to understand technology use or lack of use during hurricanes. Due to human subjects biases associated with recalling prior behaviors and intentions [38, 218], we preferred data collected during or close to a hurricane; however, actually collecting sufficient data during or immediately after a hurricane would have been logistically improbable and potentially dangerous and unethical for both researchers and participants due to the physical limitations of extreme weather. We thus chose to deploy a suite of three modularized, related online surveys—one retrospective over a long time at the start of hurricane season, one during a hurricane, and one retrospective after Hurricane Ida, the most destructive hurricane of the 2021 season in the mainland United States—as a mechanism that was safe for the researchers, logistically viable to implement, and that allowed us to quickly prescreen for specific and diverse geographic locations. We also chose online surveys because participant safety was paramount and online surveys allowed participants to complete the survey from anywhere, on any device, at any time, and, importantly, over any amount of time, which might have been important if they were experiencing a hurricane and needed to stop in the middle (and we discuss further ethical and safety considerations in Section 5.3.6). We implemented surveys in Qualtrics and recruited participants on Prolifc, an online survey recruitment platform[1].

We thus deployed our surveys at three types of times:

- Retrospective over 10 years of hurricane experience (**Retrospective survey**, Section 5.3.3)

- During a hurricane (**During-hurricane survey**, deployed during 2021 Hurricanes Ida, Henri, and Nicholas, with people who reported directly experiencing them (Section 5.3.4)

- Shortly after Hurricane Ida (**Post-Ida survey**, deployed when major news outlets

[1] `prolific.co`

reported residents regaining electricity, with people who reported they were affected by Ida, Section 5.3.5)

The retrospective survey serves as the main source of data, with the most participants, but we used the during-hurricane and post-hurricane surveys to complement, expand upon, and corroborate the retrospective data. Each of these surveys was comprised of a subset of our survey *modules*, described in Section 5.3.2 and shown in Figure 5.2.

5.3.1 Background: Hurricanes in the mainland US

In this study, we focused on participants in coastal or coastal-adjacent zipcodes from Texas to North Carolina. Figure 5.1 shows that these areas are the mostly frequently affected by hurricanes and tropical storms in the US. These areas have also been affected by some of the most devastating hurricanes in recent US history, with 27 of the 30 most costly US mainland hurricanes affecting somewhere between Texas and North Carolina [34]. We limited participants to those in the mainland US because designing a cross-cultural and cross-language survey presents significant challenges (along with opportunities) and because the experiences of those on islands and in US territories (e.g., Puerto Rico and the US Virgin Islands) may have significantly different experiences due to different evacuation options, aid available, and infrastructure. However, we encourage future researchers to explore the communities that we were unable to include, as our work adds to an already US-centric field.

The Atlantic hurricane season runs from June 1 to November 30 [7], but most activity occurs after August 1 [214]. 2021 was an above average hurricane season, with 21 named storms, eight of which hit the US coastline [7]. We studied people during three of them—including the most destructive, Hurricane Ida—and give further detail about each below.

Tropical Storm Henri hit the US North East, making landfall in Westerly, Rhode Island, on **August 22, 2021** [269]. Henri brought heavy rain and flooding, 1-3 feet of storm surge, and left 100,000 people without power [227, 269]. Two people died [227]. Though Rhode Island and other North East states were not in our target population, we collected

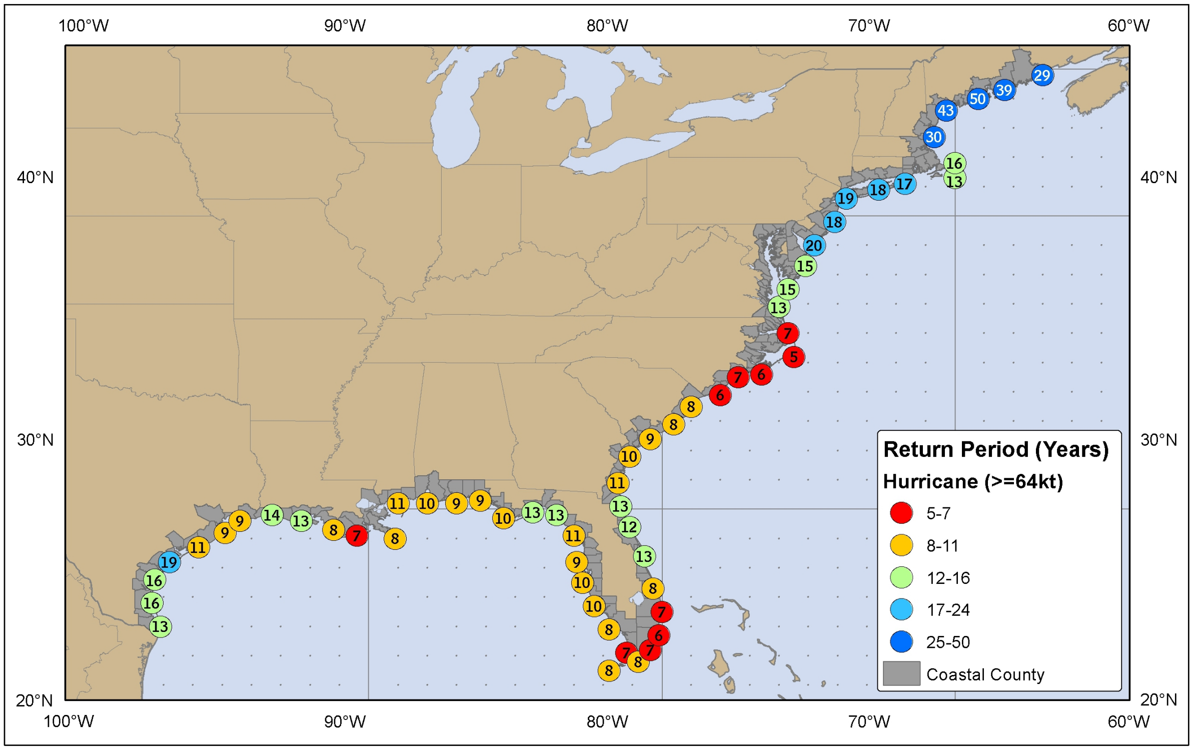


Figure 5.1: This figure from the National Oceanic and Atmospheric Administration (NOAA) illustrates where Atlantic hurricanes historically have hit the US mainland, with warmer colors indicating areas more frequently affected. NOAA's caption writes: *"Hurricane return periods are the frequency at which a certain intensity of hurricane can be expected within a given distance of a given location (for the ... images 50 nm or 58 statute miles). In simpler terms, a return period of 20 years for a major hurricane means that on average during the previous 100 years, a Category 3 or greater hurricane passed within 50 nm (58 miles) of that location about five times. We would then expect, on average, an additional five Category 3 or greater hurricanes within that radius over the next 100 years."* This figure and the quoted part of the caption are from `https://www.nhc.noaa.gov/climo/` [214].

data from those experiencing Henri as a final pilot run; we include the data here because it was high quality, but we note that there may be differences in institutional knowledge about hurricanes because the communities affected by Henri do not have much historical experience with hurricanes as the others we recruited from.

Hurricane Ida was the strongest and most destructive storm—**Category 4**[2]—to affect the mainland US in the 2021 hurricane season. **Louisiana**, where it first made landfall on **August 29, 2021**, experienced storm surges up to six feet and 150 mile per hour sustained winds [49]. As a result of Hurricane Ida, more than a million people in Louisiana lost power [1], which took weeks to restore to all [160]. Hurricane Ida traveled to the **north east** and its remnants—downgraded to a Tropical Storm—caused record-breaking rain and flooding in Pennsylvania, New York, New Jersey, Delaware, Connecticut, and Massachusetts on **September 1** [35]. Ida caused the death of at least 91 people over all the states affected [128].

Hurricane Nicholas was a **Category 1** hurricane that made landfall in eastern Texas on **September 14** and then moved east to Louisiana [177]. The storm surge was around 4 feet in Texas at landfall; measurements of rainfall vary from 4-10 inches in Texas, and were lower in Louisiana. The storm also caused "intense rain bands" in Mississippi, Alabama, and Florida, with some locations reporting 4-10 inches of rain [177]. Two people drowned, and the flooding caused property and economic damage throughout the affected areas [177].

5.3.2 Survey modules

We designed our surveys to reflect the breadth of our research questions and to allow participants to tell us something unexpected, as is standard in qualitative work. Thus, we consider our data largely *qualitative* rather than quantitative (Section 5.3.8 describes our data analysis). In order to create both consistency between survey versions and flexibility for different survey deployment contexts, we created 9 *survey modules*, described below and summarized

[2] Hurricanes are measured by wind speed using the Saffir-Simpson Hurricane Wind Scale (commonly referred to as Category 1 - Category 5); storms less than Category 1 are Tropical Storms.

in Figure 5.2. Each survey consisted of a subset of the survey modules and modified tense, question content, and survey branches as appropriate. Here we briefly describe the modules that comprised our surveys. Sections 5.3.3, 5.3.4, and 5.3.5 show how the modules fit together in the surveys—not all modules were present in each survey—and Appendix C.1 gives modules verbatim.

Disaster preparation This module asked participants about their disaster preparations—both general preparations and preparations that involved information or technology. First, we asked participants to select from a list of suggested disaster preparations that applied to them. We created this list by surveying the first two pages of non-ad Google search results for a search query about hurricane preparation and grouping together suggested items into categories (e.g., food and water, shelter, etc) [8, 26, 39, 183, 229, 283, 301, 325]. We added to this list during our pilot surveys when pilot participants indicated preparations not covered already by the list.

Next, we asked participants to select from a list of potential disaster preparations that involved technology or information. Some of these preparations—preserving paper or digital copies of documents and having alternate two-way communication methods—were drawn from the hurricane preparation guides we surveyed. Others—authentication method backups and external smartphone batteries—addressed initial hypotheses about the security and privacy implications of losing access to utilities or one's home. We also asked about apps downloaded because of the wealth of work on crisis apps in the field of crisis informatics. Finally, through a combination of free response and multi-check questions, we asked participants both about barriers to preparation and how they learned about each preparation.

Storm context This module collected data about participants' *overall* experience with a specific storm, including broad questions like "what's going on?" or "what did you and your household experience?" This module also collected data specifically about how the storm had impacted their daily routines, how their access to utilities had changed, and their expectations and concerns for the near future. The data collected in this module is critical for two reasons: (1) it shapes our understanding of participants' technology use, and (2) the questions in this module serve as prompts to help participants recall the specifics of the storm. People do not always accurately recall autobiographical events, or do not always recall all relevant details, especially when the events happened years ago [38]. Psychology research suggests that survey designs can lessen this effect by prompting participants to first recall certain specific cues around "what happened on a particular occasion, who was involved, or where the event took place" [38].

Use of disaster kit In this module, we asked participants specifically about any changes to the items in their disaster kit, if they had one. If they made changes—adding, removing, or something else—we ask them to explain what the change was and why they made the change. This module adds data to the previous module by collecting data about storm context and helping participants recall specific memories.

Reflections on preparations This module, deployed only in the post-Ida survey, encouraged participants to reflect more deeply on how they used the items in their disaster kit, whether those items were useful, and what might have been missing.

Technology use during the storm This module collected estimates from participants about how much they used technology in a number of ways during the storm, and how that compared to normal for them. For each activity, such as "getting weather information" and "playing games" and "browse on social media", we asked participants to estimate (1) how much time they spent on the activity in a 24 hour period during the storm; (2) the name of their most-used app or website; (3) whether they were able to do as much as they wanted; and (4) whether this was more, less, or about the same as their typical use. If there was anything they said they were unable to do as much as they wanted, we then asked why, in a free-response question.

Use of apps This module helps address the question of what apps people use during hurricanes, as well as what apps people do *not* use. We asked participants to name a number of apps that they used, either in daily life or in an emergency, up to three in each of the following seven categories: weather, national or international news, local or regional news, social media, text communication, video or audio communication, and in-case-of-emergency (ICE) apps. Participants were instructed to input at least one app in one of the categories, but were not required to write more that one app overall (i.e., it was fine if they had a category with no entries). We first drew app categories from Google Play and the Apple App Store, but we refined them through multiple rounds of pilot surveys with multi-generational users with experiences with disasters.

After writing in at least one app, participants categorized the apps they had entered into three groups: (a) apps they had used during a disaster but not during everyday life, (b) apps they had used during everyday life but not during a disaster, and (c) apps they had used during both everyday life and a disaster.

Then, through a series of free response questions, we prompted participants to reflect on *how* and *why* they used apps in each category the way they did, asking questions like: "what did you use these apps for?" and "did you encounter any issues or concerns?"

Broader reflections on technology use This section asked participants to more broadly reflect on changes in and characterizations of their use of technology during a storm by asking questions like "how did your use of technology change during the storm?" We revised and added to the questions in this module after the retrospective survey to ask more specifically about the importance of technology (either as it was used, or as they wished to use it), and we were careful to craft questions that did not presume that technology use *should* be important to participants.

Information security issues In order to explore our questions about security and privacy events occurring during hurricanes, we asked participants to tell us about information security and device-access issues they experienced during the storm, whether or not they believed it was directly related to the storm itself. The retrospective survey included a short version of this module with a single broad free-response question, as pilot studies indicated many participants did not recall specific incidents from years ago (in line with [38]).

Demographics We asked participants a number of standard demographic questions, including gender, race and/or ethnicity, household income, age, and political leanings. The questions about gender and racial identities included an option to self-describe in a free response option, to be used in addition to or instead of any number of the common checkboxes we provided. We also asked for their zipcode and how many years they had lived in the area, in order to further contextualize their survey responses. All questions were optional, and we also invited participants to tell us anything else we should know about them, demographically, if the questions we asked or the prescribed answers did not fit their identity. This section appeared at the end of the surveys in order to help mitigate stereotype threat.

5.3.3 Retrospective Survey

Recruitment and screening For our retrospective survey, we recruited participants who lived in coastal or coastal-adjacent zipcodes from the gulf coast of Texas through North Carolina, since over 90% of hurricanes that have hit the mainland US have hit between Florida and North Carolina [3], and there have been recent significant and destructive hurricanes along the Gulf coast, e.g., Hurricane Katrina (2005) and Hurricane Harvey (2017). Because our survey platform, Prolific, did not automatically enable zipcode-level screening, we conducted a pre-screening survey to identify geographically eligible participants who were at least 18 years old.

Additionally, our surveys ran shortly after Prolific went viral on TikTok and gained thousands of new, young, female survey-takers [44], leading to some surveys (run by other researchers) initially reporting extremely skewed gender imbalances with over 90% female

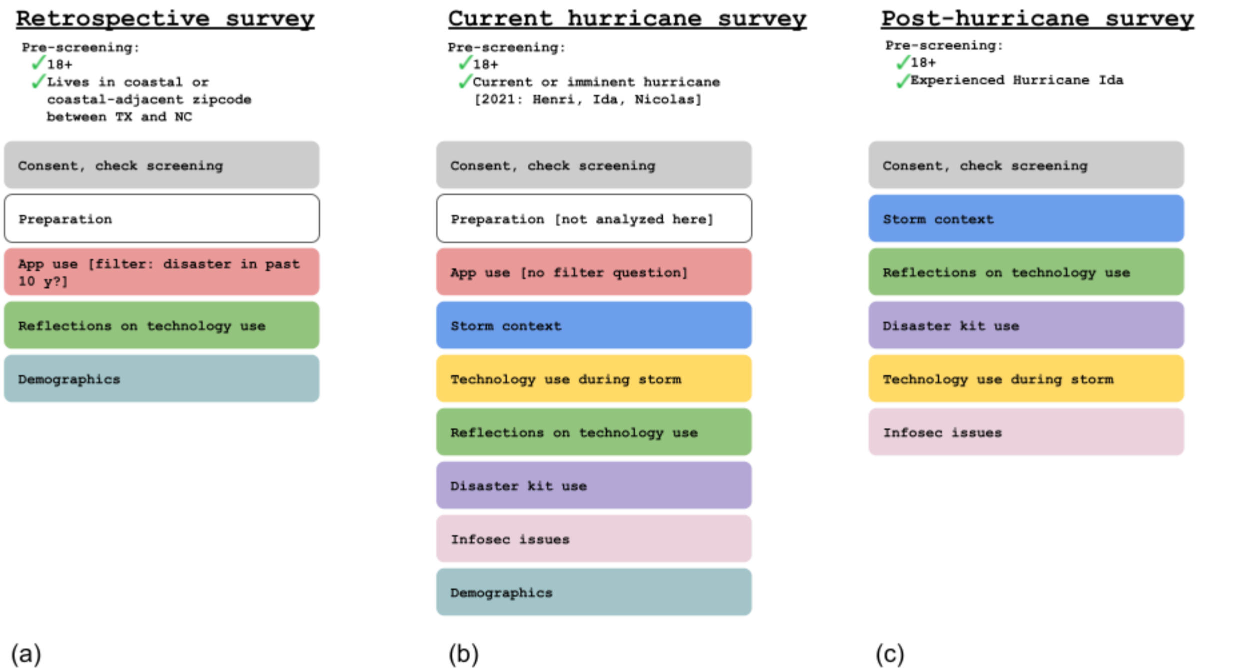

Retrospective survey
Pre-screening:
✓18+
✓Lives in coastal or coastal-adjacent zipcode between TX and NC
Consent, check screening
Preparation
App use [filter: disaster in past 10 y?]
Reflections on technology use
Demographics
(a)
Current hurricane survey
Pre-screening:
✓18+
✓Current or imminent hurricane [2021: Henri, Ida, Nicolas]
Consent, check screening
Preparation [not analyzed here]
App use [no filter question]
Storm context
Technology use during storm
Reflections on technology use
Disaster kit use
Infosec issues
Demographics
(b)
Post-hurricane survey
Pre-screening:
✓18+
✓Experienced Hurricane Ida
Consent, check screening
Storm context
Reflections on technology use
Disaster kit use
Technology use during storm
Infosec issues
(c)

Figure 5.2: Subfigures (a), (b), and (c) illustrate the modules included in each survey. See Appendix C.1 for full survey text. In reaction to results from the retrospective survey, and in preparation for collecting data currently and recently experiencing hurricanes, we revised some the modules in the retrospective survey and created new modules with more in depth questions and more contextual questions.

respondents. [3] Because of this potential for an extreme imbalance, we balanced our sample by screening equal numbers of women and non-women in a screening survey that included questions about location and gender, and then opened the survey to all participants who we screened as eligible, regardless of gender.

Survey content The retrospective survey consisted of three main parts, as shown in Figure 5.2a. Approximately the first half of the survey asked participants about their hurricane

[3] https://twitter.com/SebastianDeri/status/1423768044610854913

preparation strategies. Then, using the **app module**, for those who had experienced a disaster in the past 10 years, we asked participants about their app usage during everyday life and disasters. Then, stepping back, we prompted participants to reflect more holistically about their use of technology during a disaster in the **reflections on technology use module**, asking *how* and *why* their technology use had changed, as well as what they felt was missing and what their concerns were, including a brief question about any scams or other information security issues they or their community experienced.

5.3.4 During-hurricane survey

Participant recruitment and screening To complement the data from the retrospective survey, we additionally recruited and surveyed participants who were experiencing a hurricane or expecting to experience a hurricane in less than 48 hours. During three of the seven named storms to hit the mainland US in 2021—Tropical Storm Henri, Hurricane Ida, and Hurricane Nicholas—we screened participants via Prolific in areas that were getting hit by the storm. We asked participants whether they were being affected by the storm, including whether they were sheltering in place or whether they had evacuated (see Appendix C.2.2.1 for the text of the screening survey). If participants indicated that they were affected by the storm, we invited them, via private message on Prolific, to take part in our longer survey. We used private messages because we were recruiting participants one at a time and Prolific enforces a time limit that we did not want to give participants in case they had to stop in the middle. Appendix C.2.3 contains our recruitment message, which emphasized that participants should only complete the survey if they were safe and that we would be as flexible as possible with payment and timing. We screened and surveyed people periodically throughout the duration of storm; we stopped screening and surveying when our surveys stopped filling up with participants or when most participants said they were not being affected by the storm.

Survey content This survey expands upon the themes from the retrospective survey and adds questions to establish context and current technology usage. As the retrospective survey did, this survey began by asking participants about their **preparation** strategies, and then moved to the **app module**, which asked about apps they were using and not using during the storm. We then asked participants to expand upon what they were experiencing, both in a broader sense, and specifically about their technology use, in the **storm context module** and the **technology use during storm module**. Then, we presented them with a modified and expanded set of questions from the **reflections on technology use module** and asked them to consider what had changed about their technology use, what was most and least important, and what was missing. Importantly, we tried to craft questions that did not presuppose that they *should* be using technology. We then asked them to reflect on how they used the items in their disaster kit in the **disaster kit module** and then asked about any information security issues in the short **infosec module**, in a set of questions modified from and informed by the retrospective survey.

5.3.5 Post-Ida Survey

Participant recruitment and screening Hurricane Ida, the most destructive hurricane to hit the mainland US in 2021, left over a million people in Louisiana without power, and caused devastating flooding in the north east days later. Thus, our use of online surveys—a methodology that requires participants to have internet access and implies that they are well-supplied with electricity—did not allow us to survey those who were most affected by the storm. To partially counter this bias, when mainstream news media reported that utilities were being restored, we recruited people who had been affected by Hurricane Ida. Our screening survey asked participants how severely they had been affected, and we first recruited people who had been most severely affected (see Appendix C.2.4.1 for the screening survey text). As with the during-hurricane surveys, we stopped screening when the surveys stopped filling up.

Survey	When deployed	Avg min	Payment	# Participants	# Screened
Retrospective	Aug 23-Sept 8	21.5	$5	99	536
During-hurricane	Henri, Ida, Nicholas	24.7	$12	26	120
Post-Ida	post-Ida: LA, NYC	23.6	$5	13	63

Table 5.1: This table shows the dates of deployment, payment, number of participants, and average completion time for the three surveys. Each screening survey paid $0.25 and took on average less than one minute.

Survey content Because we were specifically recruiting people who had been severely affected by the storm, we removed the app module and the preparation modules in order to reduce the burden on participants. We asked participants generally about their experience during the storm in the **storm context module**, then we asked them to reflect broadly on their technology use (or lack of) during the storm in the **reflections on technology use module**, and then we asked them about how they had used or not used the items in their disaster kit in the **disaster kit use module**. Finally, we asked them to quantify their use of technology in a typical 24 hours during the storm in the **technology use during storm module**, and then asked broadly about security and privacy in a short **infosec module**. In an unfortunate oversight, we did not include a demographics section in this version of the survey. However, we were able to obtain information about age information as it is automatically provided to Prolific researchers; this is the demographic data we report for this survey. Because marginalized communities are historically more badly affected by natural disasters [91], it is particularly unfortunate that we are missing demographic data for this group. However, we argue that this omission does not invalidate the data due to the qualitative nature of the data and the fact that its purpose is to complement and corroborate the data from the other surveys, not to provide statistical significance.

5.3.6 Safety and ethical considerations

Ethical treatment of participants and participant safety was paramount throughout the study. We followed general best practices for online surveys of this nature, meaning that we obtained approval from our institution's Human Subjects Division (IRB), we did not collect personally identifying information from participants, we did not ask for more sensitive data than we needed, and no questions except the screening questions were mandatory. We also wrote consent text that was intentionally short but informative, lacked jargon, and gave participants a way to contact us outside the survey platform (though none did).

Additionally, we were conscious of the fact that our during-hurricane design might incentivize participants to prioritize the survey over physical safety. Though we could not verify participants' safety, we explicitly told them, both in the recruitment message and in the consent text, that they should *only* complete the survey if they were able to do so safely, and that there was no time limit. We also said we would compensate them for any portion of the survey that they were able to complete.

Table 5.1 summarizes payments and average completion times for each of the three surveys. In line with best practices for ethical treatment of human subjects, we paid participants at an hourly rate that at least matched the minimum wages in their region, and typically exceeded it. We set a high hourly rate for the during-hurricane survey ($12 for the survey, 24.7 min average) for two reasons: (a) we wanted to compensate participants well due to their circumstances, and (b) our pilot studies showed this survey would take longer, approximately 30-40 minutes.

5.3.7 Limitations

Though online surveys are a powerful tool in reaching many participants over a wide geographic area with specific constraints, they are a biased recruitment method. Crowdworkers may not be not representative of the general population; participants in their 20s are over-represented [230, 256] and may not reflect the racial, economic, political, and education demographics in their area. Recent work has also investigated whether crowdworkers' security and privacy behaviors reflect the general population, with varying results [156, 243].

By definition, our methodology excludes people who do not or cannot participant in online surveys, including people who do not have access to the internet, do not use smartphones or computers, or do not have time to complete the surveys. This means that our participants likely overrepresent those who use technology or have access to technology and connectivity in general and, specifically for the during-survey design, those who were safe enough to focus on things other than physical safety during the 2021 hurricanes. While this is unquestionably the right decision and it would have been wrong to recruit people during a hurricane who were not physically safe and able to participate, it does mean that these people are not represented in our dataset.

Additionally, non-longitudinal online surveys such as ours may not capture participants' true motivations and behaviors if the questions do not ask directly about them, as there is no opportunity to follow up with participants. Paid online surveys also incentivize respondents to go as quickly as possible in order to increase their hourly earnings, so respondents may not always give detailed or specific answers to free response questions, and may skip or be confused about long questions. However, through multiple rounds of survey pilots, and analysis of the quality of free-response questions, we believe that our survey design was sufficient.

5.3.8 Analysis

We conducted qualitative analysis on the free response answers from the surveys, using a single codebook developed by three researchers. The researchers first grouped the questions by module for ease of analysis, and then worked together to iteratively extract themes and build a codebook with hierarchical codes with 6 high level codes and 50 leaf node codes. The lead researcher acted as primary coder and coded all the data, while the secondary coder coded 20% of the retrospective data, and >50% of the other surveys (due to the small sample size). See Appendix C.1 for the codebook.

We additionally developed analysis scripts to conduct basic descriptive statistics for the quantitative data about demographics and app usage. We removed one participant's data because their qualitative responses were clearly copy-pasted and nonsensical.

5.4 Results

We now turn to our results about technology use and disuse during hurricanes. We begin with contextual results about demographics and participants' experiences during storms (Section 5.4.1), and then turn to preparations (Section 5.4.2), needs and circumstances driving technology use during hurricanes (Section 5.4.3), changes in technology use (Section 5.4.4), and coping strategies for lost access to utilities (Section 5.4.5).

5.4.1 Participant demographics and storm context

We begin by describing our participants both demographically and in terms of the natural disasters that they experienced, in order to contextualize their responses and reveal the limitations of our recruitment strategies. As shown in Table 5.1, we had 138 total participants: 99 in the retrospective survey ($R1$ - $R99$), 25 in the during-hurricane survey (D_H1 - D_H9 for Tropical Storm Henri, D_I1 - D_I12 for Hurricane Ida, and D_N1 - D_N4 for Hurricane Nicholas), and 13 in the post-Ida survey (P_I1 - P_I13). Of these total 138, 112 (81.2%) submitted short answer responses to at least one question in the survey (all questions were optional other than the screening questions).

Demographics Table 5.2 summarizes some standard demographic characteristics of our participants. As is common in online surveys [256], our participants were largely young and educated; of our 138 participants, 94 were under 30, and 89 had at least some education beyond high school. A majority of our participants–63–identified as women, with 39 identifying as men and 10 as nonbinary, with 3 reporting multiple genders. This gender imbalance is likely due to our survey platform's viral popularity on TikTok just before we recruited participants, despite our adjustments to our recruitment methods (described in

Gender (N=109)		Age (N=121)		Race and/or Ethnicity (N=112)	
Man	39	18-29	94	Amer. Indian/AK Native	3
Non-binary	10	30-39	14	Asian	14
Woman	63	40-49	8	Black/African Amer.	10
Multiple	3	50-59	2	Hispanic/Latinx/Spanish	36
		60+	3	Indo-Caribbean	1
				Middle Eastern	1
				South Asian	3
				White	56
				Multiple	12
Income (N=92)		**Politics (N=108)**		**Education (N=109)**	
< $10k	7	Democrat	82	High School	20
$10k-39k	16	Republican	26	Some college	35
$40k-59k	27			Associates	15
$60k-79k	16			Bachelors	29
$80k-99k	10			Masters	8
>=$100k	16			JD, MD, PhD	2

Table 5.2: This table summarizes participant demographics over the surveys. Due to an oversight, we did not collect demographic data other than age from the 16 post-Ida participants. Race and ethnicity categories have been slightly compressed for the sake of the width of the table (see Appendix C.1.4 for the verbatim wording). Indo-Caribbean is an identifier written in by a participant; all others were checkboxes given as options to participants. “Multiple” means that N participants are represented in more than one of the above rows.

Section 5.3.3). Exactly half of our participants who reported race or ethnicity identified as white, and slightly less than a third identified as Hispanic, Latinx, or Spanish. Black and African American participants are underrepresented in our dataset, meaning that our data may be missing contributions from minoritized groups, which are historically affected most by storms due to systemic disparities in natural disaster aid [91]. Republicans are also underrepresented in our dataset, meaning that our data is not politically representative of the majority of voters in the regions we recruited from (and because political views correlate with trust in information sources [154], a divide in political views may also affect storm preparations and technology use and information gathering during the storm).

Experiences with natural disasters We now briefly summarize our participants' experiences with storms. It is important to understand this context because these circumstances—extreme weather and damaged infrastructure—shape participants' preparations (Section 5.4.2), needs (Section 5.4.3) and technology use (Section 5.4.4), and drive some to develop workarounds strategies to fulfill their needs (Section 5.4.5).

58 of the 99 retrospective survey participants explicitly mentioned experiencing a hurricane or another major natural disaster (e.g., an ice storm), with 13 mentions of Hurricane Harvey and 8 mentions of Hurricane Irma. Due to the qualitative nature of our results, these numbers may be higher; that is, it is likely that some participants had experienced a hurricane and did not *explicitly* mention it. All of the during-hurricane and post-Ida participants were either experiencing or had recently experienced a storm.

The retrospective survey participants had collectively experienced many of the significant storms of the past ten years, including Hurricane Irma and Hurricane Harvey. Though it was outside the 10-year period we specified, $R12$ wrote that Hurricane Katrina, in 2005, "*was a nightmare. It took a year to get back to normal.*" The collective memories of these participants represent the institutional knowledge of many of the communities that regularly experience prepare for and experience potentially devastating storms.

P_I9 vividly described Hurricane Ida: "*I stayed Ponchatoula, Louisiana. We experience*

	Electricity	Potable water	Natural gas	Cell service	Internet
N=	27	23	19	27	26
avg	69.7%	75.6%	82.3%	69.4%	58%

Table 5.3: This table shows access to utilities during a given 24 hour period during a storm, from participants surveyed in the during-hurricane and post-Ida surveys. N indicates the number of data points; not all participants filled out each question or each line. Average M% means that on average, participants reporting having access M% to that utility for a typical 24 hour period during the storm. Due to low sample size, these numbers should not be generalized or interpreted with statistical significant; we present these numbers as context for understanding participants' responses.

very extreme weather, with winds at 80 mph and wind gusts up to 150mph. While i was sitting in the house, you could hear the trees snapping in half and we would just hold our breath to see where they landed. You could feel the ground shake when they fell. We lost power and cell service around 9 PM that night. We had 20 trees down on the property. We drove around town the day after too see the damage and it was devastating. Power lines were down literally everywhere. Roofs were missing off people's houses, and places that have never flooded before, did. We finally got power after 11 days, but I still have to drive into Downtown [redacted] to get cell service. I go to school in New Orleans, and my school is still closed until further notice."

Though not all participants experienced hurricanes as damaging as Hurricane Ida, most described public services, common resources, and other parts of the community being affected—commonly, electrical and cellular or internet outages, but also closed schools, damaged and closed roads, gas, food, and ice shortages, and damaged homes. Some participants in the retrospective survey additionally described an outage caused by something other than a hurricane.

Table 5.3 shows participants' estimates of their access to utilities, for those who were currently experiencing a storm or who had recently experienced Hurricane Ida, showing a lack of consistent access to basic utilities like electricity, potable water, natural gas, and cell and internet connectivity. We did not ask participants in the retrospective survey for such detailed estimates, but issues with electricity came up for 56 of them, while 26 mentioned internet outages, 15 mentioned cellular outages, and 5 mentioned general connectivity issues. Due to the nature of qualitative data, and the fact that we did not ask explicitly about power and connectivity outages and instead let it arise organically, the number of participants who actually experienced these issues is likely higher.

At a higher level, our data is consistent with news reports that public utility outages were extraordinarily common; in the following sections, we explore how the lack of connectivity and electricity is in tension with the increased need for safety, communication, and information, and leads to changed technology use and un- or under-met needs.

5.4.2 Preparations

We now turn to our results about the role of technology and informatics in household hurricane *preparation*. We first report on participants' *general* preparedness for hurricanes and other extreme weather, with categories drawn from an informal survey of disaster preparedness guides and pilot studies [8, 26, 39, 183, 229, 283, 301, 325]. This section reports results *only* from the 99 retrospective survey participants.

The most common preparations were storing extra food and/or water (89), and preparing extra batteries, candles, or some source of external power (83), as shown in Figure 5.3. Structural preparations of their home (such as closing shutters, taking in plants) were also common (61). Less commonly, participants stocked money (29), weapons (10), materials to create a temporary shelter (22), and made plans with others (15). It is important to holistically understand *all* of participants' preparations because having basic needs like food and shelter taken care of might enable participants to think about informatic needs.

We find that preparations related to technology or informatics were also prevalent, but not as common as some general preparations: 54 participants each downloaded apps and kept smartphone batteries charged, while preparations to protect documents or information were slightly less common (40 prepared physical documents; 38 made digital preparations). Slightly fewer still (28) prepared with alternate communication methods and authentication backups (19). Though these preparations are less common than the most common non-technological preparations (storing extra food and water), our sample suggests that they are still prevalent in the millions of people that prepare for hurricanes every year.

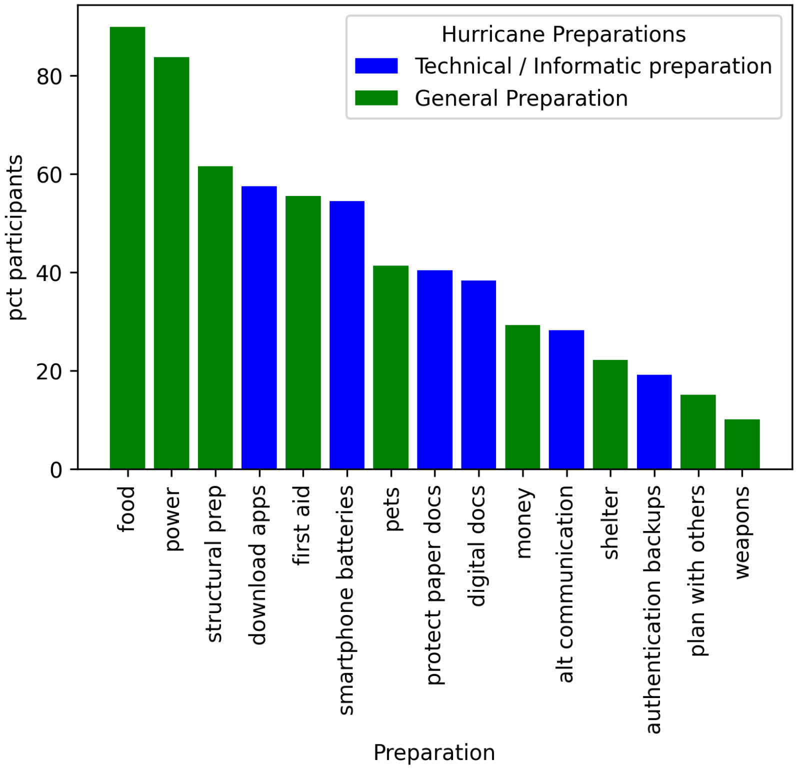


Figure 5.3: Participants' households' hurricane preparations; green categories—general preparations—are drawn from existing preparation recommendations and pilot surveys. Blue categories indicate preparations generally having to do with informatics or technology.

Preparing documents and information Hurricane preparedness guides, such as the one on the US government's disaster preparedness website, recommend saving "*important family documents such as copies of insurance policies, identification and bank account records ... electronically or in a waterproof, portable container*" [8].

The catastrophic flooding caused by hurricanes can destroy important household documents that are time consuming, bureaucratically difficult, and costly to replace. Lost identity or property documentation can lead to further issues with identity theft (if stolen and not destroyed), legal issues, or prevent one from accomplishing other important goals that require proof of identity, such as potentially receiving insurance payouts for flood damage or government benefits.

We found that 40 participants protected paper documents (i.e., storing originals or copies by their definition of secure), and 38 participants protected documents digitally (e.g., by keeping photos of paper documents). Participants qualitatively identified 22 types of document assets, most commonly, birth certificates (20 participants), family photos and videos (15 participants), and social security cards and passports (14 participants each).

Of the 40 participants who kept paper copies or protected the physical document, some used safes (18 participants), while others used physical folders (7 participants) and one used a "*private journal*". Many mentioned waterproof or fireproof storage (which many safes are); some use plastic bags to fulfill the waterproof requirement, while others used safes. Five participants specifically mentioned ease of accessibility ($R$84: "*Social security cards and birth certificates are in emergency bags in case we need to evacuate*"); others valued resilience to flooding ($R$57: "*Store it high up in a closet contained in a box of folders*"); while most mentioned physical security, i.e., a safe or secure box. Some combined measures by placing the safe in a high up or easily accessible place, like $R$82: "*We keep any vital documents (passports, birth certificate, social security card, etc.) in a safe high up so that water cannot get to it in an emergency.*"

Thirty-eight kept digital backups of documents (including digital copies of paper documents). Of those, 28 kept copies in the cloud, 10 on USB drives, 6 on an external hard drive, 3 email, and 2 on a local computer. *R*12 wrote: "*My mom keeps the digital copies of our documents on google drive and we have pictures of everything on our phone.*"

In these strategies for securing information digitally and physically, we observe that some of these practices reveal both tensions and alignments between physical security and digital security, revealing gaps in participants' knowledge or access to technology, as well as gaps in technology design and developer threat modeling. For example, while storing paper documents digitally may allow users to make the preservation more robust against physical threats like floods (e.g., by putting that copy somewhere on the internet through email or on the cloud, or by making it easily accessible on a hard drive), it may also open users to security risks and harm if there is a data breach or if someone gains access to their account (legitimately or not). Indeed, two participants rely on other people as trusted parties to keep documents safe—*R*97 stores "*personal documents with my family in places that don't have natural disasters,*" and *R*6 "*email[s] the docs to myself and family members.*" This tension between physical information security and digital information security manifests differently for people depending on their vulnerability to flooding and structural property damage, which varies by location and finances. The variety of both digital and paper preservation techniques is striking; while participants mentioned adapting their physical protections to their physical threat model for the storm and their own home, these same kinds of reasons were absent from their choices for digital copies. As we discuss in Section 5.5, the burden to close the gaps between practices that address the physical security threats from natural disasters and practices that address cybersecurity threats lies largely on *designers* and *technologists.*

Apps downloaded in preparation for a storm Smartphone apps can be a specific tool to use in preparation for, during, or in the recovery period of a crisis, as discussed in Section 5.2. Just over half of our participants (54) said they had downloaded one or more apps in preparation for hurricane season. Despite the many types of emergency apps available, the 54 participants who had downloaded apps overwhelmingly identified weather tracking apps as apps they had pre-installed in preparation for a weather emergency, with

57 mentions of weather apps. There were 13 mentions of news apps, nine mentions of maps or navigation, and eight mentions of alert apps, including four mentions of the FEMA app. One participant said they downloaded apps for identifying plants "*in case for some reason we have to bunker down in the woods and need to forage*" ($R$97). We return to the use and disuse of these apps *during* hurricanes in Section 5.4.4.

Preparations enabling access to technology or the internet In addition to asking about apps downloaded and preparation of information, we also asked about other preparations involving access to information technology, involving smartphone batteries, backups of authentication, and alternative communication devices. While these preparations were slightly less common amongst our participants, they reveal how infrastructure (or lack of reliable infrastructure) can incentivize individuals and communities to adopt certain technologies, and they also underscore the importance of *community* in recovering from a disaster. As we discuss in Section 5.5, the prevalence of preparations to enable *access* to technology or the internet also raises questions about whether the technology users are trying to access is designed to be run in a environment with either little access to electricity, little access to bandwidth, or both, and what role technology can or should have in reacting to unreliable infrastructure.

Twenty-eight participants' preparations included some form of alternate connection or communication. Most common were WiFi hotspots (19 participants); $R$50 had "*an external WiFi source so that in the case we don't have power, we are able to connect to the internet to make phone calls or text.*" Eight participants had Walkie Talkies in their emergency kits, e.g., $R$9, whose family has "*multiple Walkie talkie that we give our neighbors to use so we can communicate if we don't have any phone services or ran out of battery.*" Six participants had two-way radios, and 1 participant mentioned a satellite phone "*in case I need to make emergency calls and all cell towers are down*" ($R$79).

Participants identified several reasons that having an alternate form of communication was critical to them, including a lack of cell service or internet, lack of power or drained cell phone batteries. Some specifically wrote that the alternate forms of communication (e.g., Walkie Talkies, satellite phone) was important in case of an urgent emergency during an outage ("*We have real walkie talkies incase of a big emergency*" (*R*96)); others indicated more generally that it was important to connect with others, e.g., neighbors. In Section 5.4.5, we further discuss the impact of downed infrastructure and return to the use of these preparations.

5.4.3 Needs and circumstances driving technology use during hurricanes

To further set context for the following sections about technology use (and lack of use), we explore now individuals' general, informational, and technological needs *during* a hurricane. In line with prior work on how individuals respond to disasters [115], technology use revolving around physical and psychological **safety**, **information** about the local situation, and **communication** with others arose in our dataset. Indeed, prior work has found that usage of Twitter and other social media can help fulfill these needs during crises [247]. Here, we examine how these needs drive technology use and disuse as a whole.

Perhaps unsurprisingly, much of participants' technology use was driven by the need for **weather information** (70), to track the storm before, during, and immediately after it affected their area. Some participants mentioned specifically *detailed* weather information, such as *R*70, who sought out local news for more detail: "*[I use local news for] seeing the weather that doesn't show on default apple weather app.*" Accuracy also drove participants' choice of app; *R*96 wrote that they used Clime "*to track the oncoming weather via radar for a more accurate sense of what was going to happen.*" Though it is not surprising that participants sought weather information during a hurricane, we report this data to underscore the importance of weather information through the volume of responses about using technology to seek weather information.

Participants also commonly sought information about their **local community** in the aftermath of the storm (39) or just answered generally about **staying informed** or updated (51). P_I131 wrote: "*once we would get enough service [technology] was used a great deal* *to check in with family and get updates on the town and restoration of the basic needs.*" Goltz et al [115] write about how information gathering is a critical step in the disaster recovery process; our data supports this broad need, and—as with weather information—highlights the importance of the need. Further, as we discuss in Section 5.5, the volume of people seeking weather and community information—and relying on it to make potentially safety-critical decisions—means that social media and weather apps or websites, may be safety-critical infrastructure during a natural disaster.

Some participants expanded upon their need for local information and tied it to immediate and **physical safety** or comfort needs. 10 participants wrote about using technology to fulfill basic needs like food and water, and 12 wrote about using it to find information about longer term disaster assistance (e.g., through FEMA, or local authorities). $R91$ wrote that their "*local news, WECT, was keeping everyone up to date on where to go for gas, ice, and other supplies as well as updates on storm recovery.*" Other participants relied on their phones for emergency weather advisories and warnings, like $R18$, who wrote that they relied on emergency alerts for "*extreme weather cases where I need immediate emergency information about what is happening in my area.*" In an extension of physical safety needs, participants also considered their need to call for emergency help (9). P_I138 wrote that "*in a serious flooding situation, I would need to call for help with my exact location. There's an app I keep on my phone called 'what3words' that allows for location within a few feet.*" 4 participants mentioned using technology to help them either plan or execute an evacuation, including by finding routes and digitally preparing documents.

The need for **entertainment** (20) and **psychological safety** (12) also drove participants' technology use and disuse. $R1$ wrote that they avoided "*news websites ... because they tend to make you more scared of the situation,*" while for others, news and social media sites provided comfort or a distraction. $R68$ wrote that they used "*Reddit to have a distraction from what the disaster situation wa[s],*" and some of the during-hurricane participants, when asked how their experience would change if they were unable to use technology, wrote about technology as a source of comfort and safety: "*I would have had much more anxiety* *and a lot more boredom. We also would not have been able to find emergency housing for our pet*" (P_I129).

As an umbrella over many the previous needs, **communication** with others was a massive driver of technology use, with 55 participants mentioning communication generally, and 19 further writing that they used technology as a way to either check on others' safety, or to communicate their own safety to others. Participants communicated with friends and family both in the area and far away, and often did not specify in their survey responses who exactly they needed to communicate with. As Goltz et al write, checking on loved ones is a common stage of disaster recover [115], and the volume at which participants mentioned communication as the reason they were using an app shows that this reasoning is present in our dataset as well. Speaking to the connection between communication and all other needs, particularly information needing and psychological safety, P_I10 wrote that if they had not been able to use technology "*I would not be able to get in touch with people & feel assured when I did so.*"

Finally, participants mentioned **financial security** or **schoolwork** when the storm impinged upon it (21). Both a lack of connectivity and physical damage or restrictions on the community prevented participants from doing work online at home or going to work. P138 wrote: "*I'm self-employed online. Because I was trying to save battery power on my phone, I only used it to connect with my loved ones and friends and couldn't work.... I lost 8 days of income; I had some money in the bank, but couldn't access an ATM, so my rent was late to my landlord.*" P_I13's quote reflects themes in others' responses of prioritization of safety and rationing resources, and speaks to the complexity of the changing needs driving technology use as well as the different physical and technical constraints present during a natural disaster, which together can directly and indirectly harm participants physically, emotionally, and financially.

Additionally, in response to a question specifically about **security and privacy** concerns or issues, 40 participants brought up experiences with or fears of price gauging, scams directed at people recovering from natural disasters (e.g., fake roofing companies), misinformation, and loss of important documents. These broader security concerns touch on the connections between financial security concerns and digital security and privacy concerns; in Section 5.5 we explore this connection more deeply.

5.4.4 (Changes in) technology use during a storm

We now turn to the specific technologies that participants reported using—and not using—during the storm, as well as why and how this model of usage represents a change from everyday usage. Figure 5.4 shows the apps that participants used and didn't use during the disaster as well as during everyday life, as driven by the needs explored in Section 5.4.3. Figure 5.5 additionally shows app usage by category, and Table 5.4 shows the apps or technologies that participants wrote in each categories.

Social Media: useful but a massive power drain As shown in Figure 5.4, Twitter, Facebook, and Instagram dominated participants' social media usage overall. Figure 5.5 shows that participants indicated use of social media apps during disaster 117 times (72 participants). Of those, 8 instances occurred *only* during disaster; separately, 26 participants indicated 66 instances of apps used specifically *not* during disaster, meaning that about half of the participants who used social media stopped using it during a disaster, while only 6 had one or more social media apps that they used *only* during a disaster.

Participants' reasons for using social media during the storm echoed the greater driving needs during the storm, explored in Section 5.4.3. For some participants, social media was a critical part of disaster recovery, aiding in situational awareness about the weather and the local impact, as well as communication with loved ones. D_N1 wrote that they "*use social media to know about my surroundings, friends posting how bad is in their area, to know about communities that might need help, to know when is the storm going to pass.*" $R9$ also used social media apps (in addition to others) for communication, and added that these apps were critical for relaying messages: "*I used Snapchat, Facebook, iMessage to stay in contact with friends and family out of area. Also used these apps to relay messages and keep up with info*

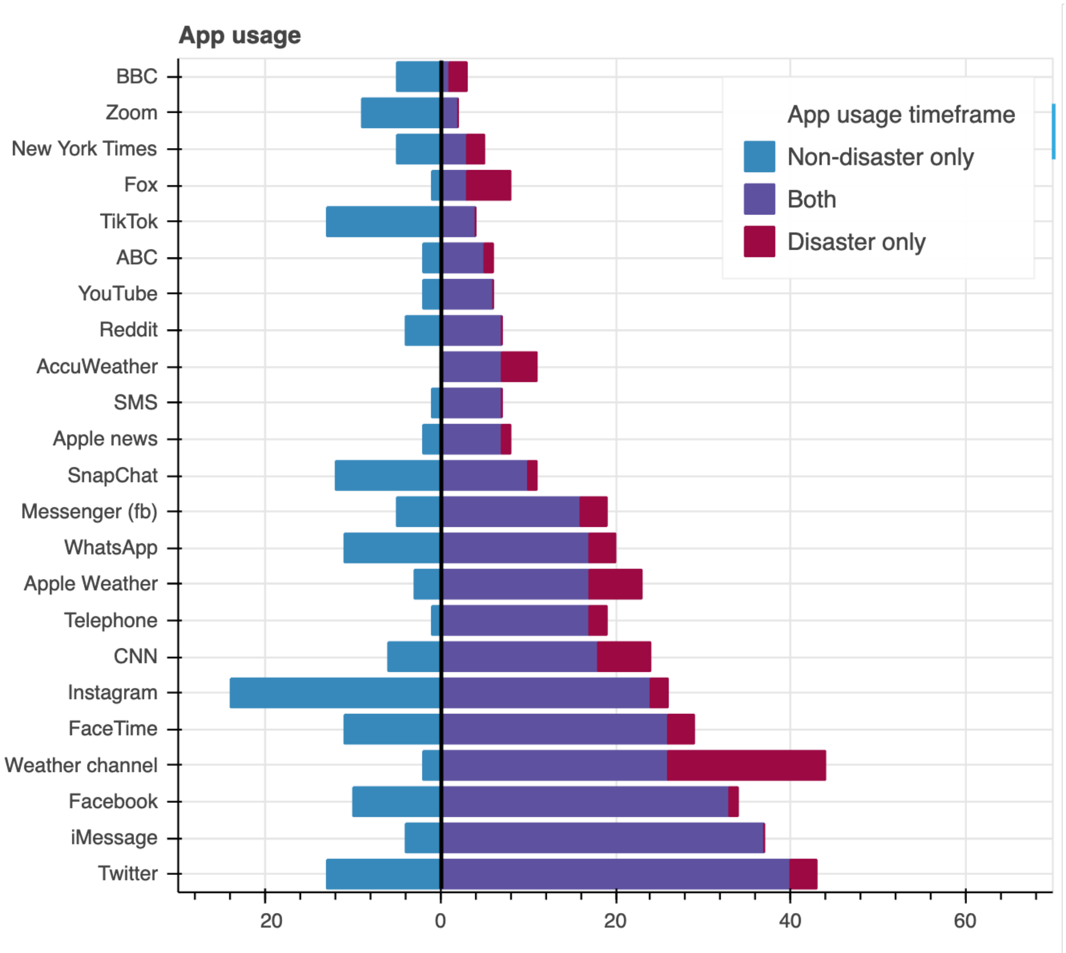


Figure 5.4: This figure shows which apps participants reported using during disasters only (red), never during disasters (only everyday use) (blue), or both during disasters and during everyday life (purple). News sources are counted as national news by default, or local news if given a qualifier like "ABC channel 12" or "FOX 7." Note that we assume that "weather channel" refers to the company "The Weather Channel", which is the same as `weather.com`

from those also experiencing the disaster." D_I6 also used social media for "*entertainment purposes*" as well as "*communicating with friends and relatives.*"

Participants also wrote about the utility of social media in crowdsourcing local information immediately after the storm, both to share information and to find or give assistance, as

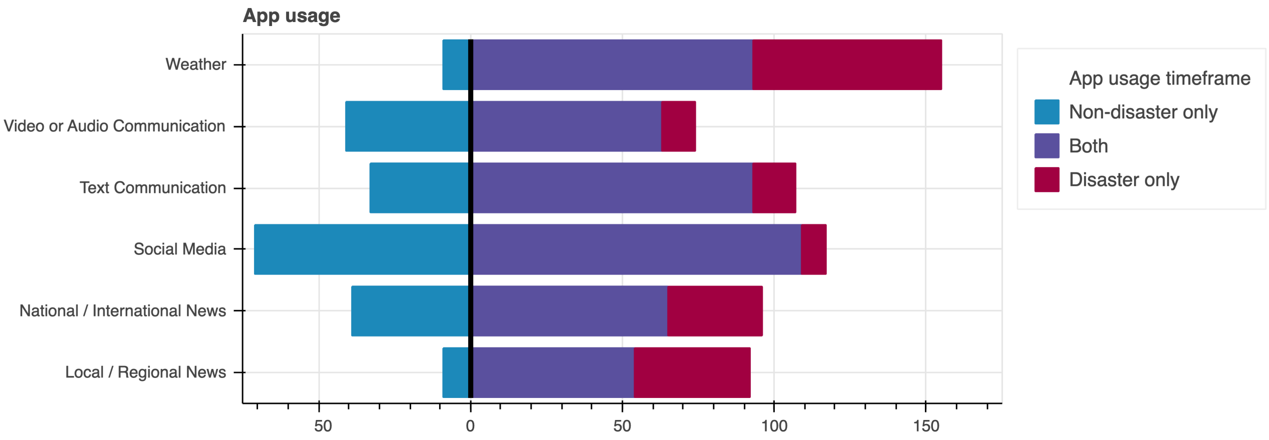


Figure 5.5: This figure shows which categories of apps participants reported using during disasters only, never during disasters (only everyday use), or both during disasters and during everyday life. News sources are counted as national news by default, or local news if given a qualifier like "ABC channel 12" or "FOX 7."

prior work has explored, e.g., on Twitter and Facebook [247, 273]. $R7$ explained that "*Reddit has been a great source in the aftermath of storms because there's so many people from different communities sharing information with everybody. You can usually find information about power outages, relief funds, food offerings, etc in real time.*" Additionally, $R18$ used social media to offer help to others, writing that "*during the recovering period, social media apps and apps to stay connected to people were mostly used to put the community back up. I used it to find harshly hit areas in need of supplies and to contact friends in need of help.*"

Different social media communities and apps may be useful at different stages in the disaster process; participants in our study most frequently said they found Twitter and Facebook most useful, in line with prior work [247, 273]. $R94$ distinguished Twitter as "*ridiculously useful for quick updates both from official accounts and people locally sharing videos and updates,*" but wrote that "*Facebook is good for checking in on the local community after the danger passes or seeing what mutual aid efforts are going on.*" $R65$ added that "*facebook and instagram arent exactly the best at providing news updates, twitter is a social media platform much better suited to that.*"

However, as shown in Figures 5.5 and 5.4, many participants actually stopped using social media (some more than others) during the disaster, despite the communicative, entertainment, and informational value. Many participants cited battery drain or lack of connectivity as a reason to ration or completely stop social media usage, like $R1$, who wrote: "*I don't use TikTok during an emergency because I need to conserve my phone battery....*" $R14$ explained that they used the apps for entertainment and did not mention the values echoed by other participants above, writing, "*I use these apps for connecting socially but not in direct communication. I didn't feel the need to use these apps for entertainment at the cost of depleted energy stores.*" Finally, multiple participants expressed that it was "*not important to be checking ... social media during serious times*" ($R17$), and thus, they deprioritized social media. $R14$, for example, had other ways to connect with family during the storm and thus did not need to use social media—"*My family usually just commincates through text messaging so I don't need to use social media to contact them during a disaster.*"

Thus, participants expressed two stories of social media usage: one in which social media is a critical tool in communicating, crowdsourcing, gathering information, and maintaining emotional stability, and another in which the value that social media would bring to them is not worth the battery drain, or they do not find it important. People use or don't use social media in different ways, and our goal in here is not to argue for one usage model over another; however, we observe that many of those who stopped using social media did so because the power draw of the app was not worth the value they perceived in the app. In Section 5.5 we discuss some potential policy and technical recommendations with the goal that social media users should be able to decide to use the platform based on the value, not based on the value as a function of power draw.

Video, Audio, and Text communication tools Next, we discuss communication tools, grouping together video, audio, and text communication tools because they sometimes overlap. As shown in Figure 5.5, direct text, audio, or video communication tools—like iMessage, Skype, or a telephone call—roughly echoed the usage of social media: a considerable amount of disaster use, some of which was only during disasters, but a clear drop-off of usage during disasters. Disaster usage was high: 55 participants identified 74 instances of video/audio apps they used during a disaster (e.g., FaceTime); 78 participants identified 107 instances of using text communication apps during a disaster (e.g., SMS). However, 30 participants noted 41 instances of video/audio apps that they used in everyday life but *not* during a disaster, and 26 participants recorded 33 instances of text apps also not used during a disaster. We summarize apps with more than 5 mentions in Figure 5.4 and show all app mentions in Table 5.4. Broadly, this data shows that participants stopped using video/audio tools more than they stopped using text messaging apps, but it also shows an additional skew present in our dataset: 51 participants said they used FaceTime, Apple's built-in video chat app, showing that our participants had a high rate of ownership of Apple devices.

Participants identified messaging apps as critical to their communication strategies during the storm, sometimes in combination with social media. Participants emphasized the importance of being in contact with loved ones both to check in on them and to let them know that they themselves were safe (or needed help). $R26$ "*texted family members and friends let them know we're okay or ask how they were affected*" and $R14$ added that they used "*Facebook, Facebook Messanger, Facetime, and Whatsapp ...to update friends and family as well as communicating plans and coordinating any required relief.*" D_N2 said that their text and audio increased—"*I spent more time calling and texting family than usual in order to give and get updates on the state of the storm*"—and $R7$ "*used facetime to see video footage of the actual storm and its damage that it caused.*"

As revealed in Figure 5.5, many participants stopped or decreased use of video or audio tools during the storm. As with social media, for many, this change was due to the drain on battery life ("*Video greatly reduces battery life*" ($R98$)). D_I11 explained that even those who were still connected to municipal power might ration power usage in case of a future blackout: "*I am not using the zoom app since I need to reserve my battery power and online* *use just in case of power loss.*" Other participants cited the need for strong cellular or internet connectivity required by many connectivity tools, and explained that their connectivity throughout the storm was not sufficient. P_I5 described their cellular connection throughout Hurricane Ida and how that affected their ability to communicate with loved ones: "*I could communicate normally for the initial part of the storm on Sunday evening. Around ∼10 PM, I lost LTE, and then dropped down to 4G, and then just bars. I could send SMS messages, but not iMessages, on AT&T. I woke up Monday morning around 9/10 AM and had no service. Around 4 in the afternoon, calls and SMS texts would come through sporadically, but often had to be resent or attempt multiple times for the call to come through. I had more or less normal cell reception by that evening, although it felt slower than normal.*"

Finally, participants also expressed the idea of *prioritization* of certain communication tools, often the ones that cost less power and bandwidth. D_I10 wrote: "*I don't need to FaceTime or Zoom anyone. As long as I can hear their voice, I'm fine. All the people that I need to check on and care about have my actual phone number, so I don't need TextFree.*"

These usages reveal a duality similar to social media usage and speak to the need for detailed, up-to-date, and accurate information about the community and loved ones explored in Section 5.4.3 and prior work [115], but dampened by electrical and connection outages caused by downed infrastructure.

News: local news use rises during disasters Though social media and messaging and video apps can fulfill one's needs, many participants also indicated use of news apps or websites, as shown in Figure 5.5. We find that both local and national news usage increases during a disaster, but local news usage increases more: 76 participants mentioned 92 instances of local news sources used during the disaster, with nearly half of the instances (44) being used *only* during the disaster. 67 participants mentioned 96 instances of national news during the disaster, and 25 of those participants said they used 31 instances of apps during *only* the disaster.

However, many more participants indicated that they *stopped* using national news during the disaster: 25 participants identified 39 national news sources that they had stopped using the disaster, while only 7 participants indicated 9 local news sources used only during the disaster. Indeed, D_H8 wrote "*i have been watching the news more than i would normally.*" We next explore why participants turned to local or national news, and note that these results point to the critical importance of local news organizations as a source of detailed, accurate, and up-to-date information for many during a natural disaster—some using local news alone, some in complement with social media or communication tools. Participants identified approximately 65 unique local news organizations,[4] which includes apps, websites, television channels, and radio stations—anything they chose to categorize as local news.

Echoing general themes about the kind of information people need, participants preferred news sources that were accurate, timely, and detailed, both about the storm itself and the recovery process; for many, this was their local news outlet. D_I10 used their local news because they had "*a storm tracker that I'm using and [they] are constantly giving updates on the hurricane.*" $R74$ added that their local news station had more detailed weather information than their standard weather app; they used it for "*seeing the weather that doesn't show on default apple weather app.*" During the recovery period, $R62$'s local news "*gave instructions for fema and for local places giving ot supplys like food ,ice...gas..and tarps.*" Speaking to the need for physical safety, some additionally turned to local news to check on local mandates and official warnings or orders, like $R14$, who used their local news app to "*see if there was any local mandates we needed to know about.*"

While most participants agreed that local news was an important part of their information diet during the disaster, participants were split on the utility of national news. Some valued national coverage of the disaster, like $R91$, who "*used CNN to see what was being shown nationally about the disaster,*" while others did not find national news organization had the level of detail and timeliness that they needed: "*Reddit, CNN and BBC don't have the local*

[4] This number is approximate because some participants made ambiguous entries, such as "local news" or "channel 10." We did not count non-specific entries like "local news," and we counted channel 10 as its own local news source that could, for example, overlap with something like "KHOU."

#	Social Media	#	Text Communication	#	Video & Audio Communication
62	Twitter	54	iMessage	51	FaceTime
61	Instagram	34	WhatsApp	14	Zoom
56	Facebook	23	Messenger (FB)	12	WhatsApp
21	TikTok	11	Messages	8	Skype, Telephone
18	SnapChat	9	SMS	7	Discord, Messenger (Facebook)
10	Reddit	7	SnapChat	6	SnapChat
7	YouTube	6	Gov alerts	4	YouTube, Google Duo
2	WhatsApp	5	Telegram	2	Radio, Line, Zello
1	Discord, Gab, Telegram	3	Line, Instagram	1	Boss, Facebook, Fox, Instagram Marco Polo, Microsoft Teams, Oovoo Teams, Telegram, TextFree, TikTok Walkytalkies
		2	Facebook, Discord, TextNow, Signal, GroupMe, Zello		
		1	WeChat, TextPro, Text me, TextFree		

#	Weather	#	National News	#	Emergency technologies (ICE)
39	Weather channel	39	CNN	12	911
34	Apple weather	14	Apple News	11	Telephone
18	Local news	11	New York Times	6	FEMA
12	Accuweather	10	BBC, Fox	5	Emergency Alerts, iMessage
10	Weather.com	9	ABC		
6	Google, Weather Underground	8	Google, local news	4	WhatsApp, Zello
5	NOAA	7	NBC, Twitter	2	FaceTime, ICE - In Case of Emergency app Radio, Red Cross, Twitter
4	National Hurricane Center, WeatherBug	5	NPR		
		4	Associated Press, Reddit		
3	Hurricane Tracker, Facebook, National Weather Service	3	MSN	1	Apple Notes, Bank app (unk), Broadcastify, Citizen, Clime, CNN, Compass, First Aid, Flashlight, Gas finding app (unk), Gmail, Google, Google maps, Google offline maps, Instagram, Invisawear, iOS emergency, Life360, Local emergency website, Local news, Maps (unk), maps.me, Noonlight, phone app for 911, PictureThis, Pulse Point, Ring, Severe Weather Alerts, Storm shield, Text Now, Waze, Weather.com, Wells Fargo, 211
		2	Facebook, NewsBreak, Telemundo, NewsBreak		
2	Clime, Dark Sky, MyRadar, Space City Weather, Storm Radar, weather.gov				
		1	Axios, Buzzfeed, Citizen, Daily Mail, Drudge Report Estrella, The Guardian Instagram, Morning Brew, Newsplace New York Post, USA Today, Reuters, TV, Washington Post, YouTube		
1	ABC Weather, Apple News, CNN, Critical Weather, Emergency Alerts, FEMA, Instagram, Microsoft Weather, Max Hurricane Tracker, My Hurricane Tracker, MyWeather, RadarScope, RadarTracker, RZ Weather, Storm Stracker, Univision, Weather Alert, Windy, 1Weather				

Table 5.4: This table shows the number of participants who wrote in each app name in each category. For “Messages” in the Text Communication category, it is ambiguous what exactly participants—we hypothesize that it refers either to Android or iOS’s built-in messaging apps.

coverage, in real time, that I was looking for." D_I4 additionally wrote how they trusted their local news to be more accurate simply because it was local: "*I tend to trust my local news and politicians to keep me up-to-date than national news. They are not experiencing the hurricane in New York.*"

Participants' appetite for accurate, detailed, and timely information about their local area drove them to adopt use of local news apps during a disaster, as shown in Figure 5.5. As we discuss in Section 5.5, this notable increase in use of local news points to the critical role of local news in a disaster.

Weather apps: variety and high adoption Consistent with the driving need for weather information, participants indicated extremely high usage of weather apps or websites, and additionally indicated high *adoption* of new apps or websites for the storm. As shown in Figure 5.5, 110 participants identified 155 instances of weather tools they used during the storm, with 42 participants indicating that they news began using tools in 62 instances. Participants indicated 36 unique sources of weather information; additionally, 16 people wrote local news sources, and one person wrote in Instagram as a source for weather information.

Echoing themes from why they used news and social media apps, participants preferred weather sources that had detailed, accurate, and timely information, and specifically mentioned weather information as being critical immediately before and during a storm. Speaking to the importance of weather information for proper preparation, D_N1 wrote that they "*use the Weather App to know more exactly when is it going to rain and how much precipitation we are going to have, just to prepare.*"

As reflected in Figure 5.5, many participants downloaded or started using *new* apps or other sources of information specifically for the storm. $R16$ "*downloaded the local weather app as advised from the local weatherman,*" speaking to the potential influence of local news on technology use and information consumption. $R96$ explained that proper storm preparation was critical, and that for them, it was important to have multiple sources of weather information and forecasts. $R96$ downloaded "*more weather apps so that I could get the most accurate idea of what would happen weather wise during a disaster, just because I found only having one app to rely on for weather was bound to get you mixed up sometimes and either over-prepping or under-prepping.*" Underprepping could have physical safety or financial consequences (e.g., damage to personal property, loss of ability to work), while overprepping could also have financial and personal consequences if one unnecessarily evacuates or spends money on preparations that will go to waste.

Participants also explained that they stopped using weather apps—and local news—when the storm was over and the need had subsided. $R37$ wrote that "*once things started looking up, I stopped using the weather apps/local news app on my phone.*"

The pattern of reliance on both weather and local news apps as well as the volume of adoption of new apps or information sources points to the critical importance of weather information sources—as with local news—during impending natural disasters. In Section 5.5, we explore the idea of weather and local news apps as critical infrastructure during a natural disaster.

In-case-of-emergency (ICE) technologies Finally, we turn to apps that are specifically built for emergency circumstances, referred to here and in crisis information apps as ICE apps. In our survey, we very loosely defined ICE apps and let participants write in whatever *they* thought fit, so some participants wrote in '911,' i.e., the phone number to call for emergency help in the United States, and others considered emergency alerts to be an ICE technology (we do not disagree). 56 participants wrote in 71 instances of ICE technologies used during a disaster. Because personal emergencies can happen at any time—including during a natural disaster—we do not report data split by when participants used them and instead focus on what technologies participants used and why.

13 participants mentioned 911 and 7 mentioned regional emergency alerts, which may come in an app, a text, or an emergency message broadcast to all phones in a region. 6 participants used the FEMA app and 2 had the Red Cross app—both apps by national or

international organizations that help with storm recovery and emergency alerts. A handful of participants had bespoke ICE apps to help them send out personal information or detailed location information, presumably if they needed to be rescued. $R51$ had the app Invisawear "*to send emergency contacts my location*" and P_I13 prepared by downloading the app what3words: "*in a serious flooding situation, I would need to call for help with my exact location. There's an app I keep on my phone called 'what3words' that allows for location within a few feet. Assuming I could keep the phone dry and operable, I'd use that for sure.*" Other crisis apps included My SOS Family, Pulse Point, Life360, FirstAid, and Noonlight. Another participant wrote in the iOS emergency feature. Prior work has explored how people use social media to supplement the existing emergency phone system (911) when it goes down during a disaster [328, 332].

Though they aren't typically considered ICE apps, some participants mentioned map apps, such as Google Maps or the offline map app maps.me as critical to finding evacuation routes or safe driving routes when cellular infrastructure was impacted by the storm. $R14$ wrote "*We didn't have internet and cell service was spotty so we used maps.me for navigation.*" Other participants wrote in news and weather apps. Multiple participants wrote in communication tools like "telephone" and "iMessage" and "WhatsApp." Two participants mentioned apps to listen to emergency services activity: Broadcastify and Citizen. Four participants wrote in either analog technologies or apps that replace analog technologies: Flashlight, compass, and radio (2). The inclusion of these general-purpose apps and technologies points to their importance in emergency situations and highlights the criticality of developing regular apps with low-resource contexts in mind, as we discuss in Section 5.5.

The variety of entries in this category indicates that our question could have been more clearly about apps made *specifically* for crisis use (like FEMA and Noonlight). However, the apps in this category are an interesting look into what participants considered *their* emergency go-to: for one person, it was local news; for another, it was Noonlight, an app that can trigger a call to emergency services with pre-filled information. We observe that there are few bespoke crisis apps in this list and, in Section 5.5, discuss how this data may direct future research and development resources either towards encouraging adoption of these apps or discovering why they are not being adopted.

5.4.5 New strategies or models of technology use that emerge due to downed infrastructure

Finally, we turn to *new* models of technology use adopted specifically because of electrical, cellular, and internet outages, which are common during hurricanes and other natural disasters. It is important to study the patterns of technology use that emerge in the resource-constrained and physically dangerous environments caused by hurricanes because these new strategies fill gaps left by technology largely designed for a different use case, and a lack of strategies signifies systemic barriers.

Power outages caused participants to ration their phone use and find alternative charging methods Power outages are extremely common during and after hurricanes and, indeed, as revealed in Section 5.4.1, many participants experienced power outages. Outages may last for several hours, days, or weeks, depending on the extent of the damage; Hurricane Ida, for example, caused power outages for nearly a month in Louisiana [160].

37 participants wrote that they decreased or changed their technology use in order to preserve their phone battery. As explored in Sections 5.4.3 and 5.4.4, some participants used apps with lower power draw, or used apps less frequently, at the cost of communication, information gathering, and psychological safety and entertainment. Recalling a bad winter storm from earlier in 2021, $R89$ wrote about how the lack of electricity left them starved for information: "*I was on my phone less, I was able to eat and bathe and stay warm through heat from the stove but I was unaware of what was going on in the world.*" Participants rationed electricity to prioritize what they needed (or expected to need) their phone the most for; for example, $R80$ explained that if their power went out, they would "*try to save my battery for needing to contact friends or EMS in case anything happened.*"

Participants described a combination of phone use rationing and alternative charging sources until electricity came back. Many participants who used alternative charging sources used external smartphone batteries, but some used their cars, and others traveled locally to find somewhere to charge their phone. P_I13, who was without electricity for 8 days after Hurricane Ida, described their principled approach to rationing the power in their external smartphone battery as well as their alternate sources of electricity: "*I allowed my power bank to discharge 10%/day to allow discharge/charge cycles of about 20-30%/day on my phone. For example, I used 30% of my phone power on Day 1, charged it back to 90% with the power bank on Day 2, used another 30%, charged it back to 80% on Day 3, etc. I tried to ration my use to no more than 10%/day on the power bank and 30% on the phone.... I managed to keep it going for 7 days, and found an alternative (a Whole Foods with electricity a few blocks away) to give my phone a couple of charges before power came back on.*"

Thus, we observe that damaged electrical infrastructure significantly constrains technology usage after a natural disaster, at times costing participants information, communication, work, and emotional health, recalling findings from Madianou et al about communities in the Phillipines [190, 191]. However, individuals are able to ration their power usage or find alternative power sources that somewhat mitigate the concerns, depending on the length of time. In Section 5.5 we explore recommendations for researchers, technologists, and policy makers to reduce the burden on those who are experiencing a hurricane.

Complete connectivity issues were largely insurmountable Cellular and internet infrastructure is commonly damaged or destroyed by storms. In contrast to power outages, where participants can ration their use of their phone battery or external batteries, there is no commercially available and affordable replacement to downed cellular and internet infrastructure.

Most participants who had no connectivity—that is, they had lost both cellular service and wired/wireless internet—did not mention workarounds. However, some downloaded offline technologies, including walkie talkies (or walkie talkie apps), local travel, and one-way radios. P_I9 described their local travel: "*I have to drive into town to get service to be able to respond to people.*" Likewise, P_I11 "*literally drove over to my in-laws house to* *ask them things...it was annoying.*" Both of these strategies depended on the individuals having safe transportation—for these participants, a car—and roadways that were clear and safe, which is not always the case after a natural disaster (e.g., roadways may be flooded or blocked with downed trees). Six participants mentioned use of a radio, which is a commonly recommended piece of a disaster kit, and can at least allow users to receive news in a low-power and low-connectivity situation.

Others used offline apps, or apps they believed were offline. Two participants mentioned downloading Zello, a walkie-talkie app, including P_I11 who "*downloaded Zello because I heard you could use it when you didn't have good phone service. I used it to communicate with my mother who was in a much harder-hit area.*" However, Zello does not actually work without a data or internet connection [104] and was the cause of misinformation following Hurricane Ida [46]. P_I6 observed: "*People were ... posting incorrect information about how the app Zello can be used when the phone lines go down. (You need a data connection or a wifi signal to use Zello, just like any other messaging platform.)*"

The use of *new* communication platforms during a critical time points to the importance of the trustworthiness and usability of the apps; in Section 5.5 we explore potential security and privacy implications of app adoption during a critical time.

Partial connectivity was largely manageable Not everyone lost connectivity completely; some lost only cell service, and others lost only internet, or retained both but experienced extremely slow connection speeds. For many, losing electricity also meant losing internet access, like $R8$, who described that they "*used a mobile hotspot for wifi and used candles for light.*" Indeed, multiple participants who retained cellular connection were able to rely on the mobile data plans for connection; $R14$ "*had access to the internet through our data plans on our phone*" and P_I4 even "*bought additional data for the month so we could stay connected, up to date, and entertained until power was restored.*"

These partial solutions point to the fact that communities *can* make do with partial connectivity, but there are costs to doing so, e.g., loss of information or communication because of deprioritization, or the financial costs or purchasing additional mobile data, or even an electrical generator.

5.5 Discussion and Conclusions

At a high level, our results show that those affected by hurricanes have varied strategies for fulfilling their needs, but they have a common set of needs, circumstances, and barriers. We believe that solutions and improvements should come from multiple communities in order to be most effective, so our recommendations are for a wide range of researchers, technologists, and policy-makers. In this section, we propose several directions for technical solutions to problems that are ultimately caused by the failure to adequately protect physical infrastructure, so we emphasize that at a high level, **policy makers** must continue to push for resources to fix and protect physical infrastructure, especially in communities that are vulnerable to natural disasters. We also stress that technical researchers and developers must consider both the importance of user consent and the potential for abuse of *any* system that prioritizes something (a user, an app, certain functionality of an app, certain network traffic, etc) over something else, even when intended for social good. While we believe that there *are* partial technical solutions to connectivity and power issues that prioritize traffic or computation, we have to be careful of introducing *more* harm through a system that can be abused or exploited by a malicious third party, or a malicious or greedy developer.

Connectivity issues can be addressed at multiple levels Participants identified a complete loss of connectivity—both internet and cellular service—as essentially insurmountable, and a partial loss of connectivity as a cause for rationing technology use and potentially missing critical information. Recent work in the HCI community proposed a flexible mesh networked app for this purpose, along with user preparation [126]; there may also be other applicable work on computing in low-resource environments in the field of ICTD. Specifically, we imagine potential networking or systems solutions to appropriately prioritize certain traffic during periods of low connectivity, e.g., if one cell tower is carrying the load for others. Future work should investigate who exactly should determine what traffic to prioritize, but we envision potential solutions at different technical levels, e.g., a network flag like the Quality of Service flag to designate critical traffic, Internet Service Provider (ISP) emergency prioritization and load balancing of traffic, or applications or operating systems flagging or dropping outbound traffic. All of these potential solutions have drawbacks and massive potential for abuse, so we strongly recommend systems and networking researchers to consider the use and abuse cases for traffic prioritization, as well as user consent.

Systems and app developers should design for low-resource contexts in order to reduce the difficulty of electricity rationing Rationing power use was a major theme in our data. We strongly recommend that apps developers consider the power draw of their app and specifically design a low-power (or low-connectivity) mode that users can explicitly opt in or opt out of. This could mean different things for different apps; for example, it could mean pre-fetching data when connected to power and not on the OS's lower power mode, lowering the quality of video and images, not showing ads, reducing or stopping automatic uploads (e.g., backups). This type of power rationing could also be done at the level of the operating system, like existing low power modes on iOS and Android, and could even ask the user to opt-in to low power mode if the area is experiencing (or about to experience) a significant natural disaster.

Moreover, we urge developers to *develop for crisis* and, specifically, to develop with low-resource and high-importance contexts in mind (which may also extend beyond crisis). Prior work shows that it may be difficult for users to adopt new communication platforms quickly during a crisis, e.g., a political revolution [66], so we emphasize that all apps should be designed with crisis usage in mind, meaning: usable during low-power and low- or no-connectivity. The makers of Zello, the walkie talkie app that multiple participants thought was usable offline, and that now (as of April 2022) advertises itself as "*ideal for emergency and disaster events*" wrote on their blog that "*Zello's role of communication in natural disasters was never anticipated when we created the app*" [310]. We urge *all* app developers to design for crisis contexts, because users should be able to use their normal suite of apps to fulfill their needs, and crises can happen to any user at any time. We also note that crises can include *adversarial contexts*, so part of developing for crisis is considering a wide variety of threat models, but that is out of scope.

The technology and information sources that people commonly use during natural disasters and other crisis events should be treated as safety-critical infrastructure. Weather, social media, local news, and others can provide safety-critical information or at least information that people need to make decisions off of. As discussed, it is important for the developers to create technology that matches the low-resource use cases of a natural disaster, but it is *also* key that we treat these technologies and information sources as safety-critical during a disaster and that we threat model appropriately about potential adversarial interference, either through a buggy app or a malicious developer. For example, popular local weather websites or social media accounts of local officials or others well known and trusted in the community might become high value targets during a crisis, if an adversary wanted to disrupt disaster aid and recovery programs, extract money from the target, or harm people in the affected communities physically and financially with disinformation. Indeed, many groups have studied post-crisis misinformation on social media, but our recommendation is to go further and consider harms and avenues of attack beyond misinformation on social media.

Additionally, the diversity of local news and weather information sources suggests that users *do* adopt some new technologies and new information sources in preparation for and during crises, and also point to the importance of having quality and well-funded and well-trained local news and weather sources.

Researchers should continue to study both technology use and the barriers to or gaps in technology use in stressful and low-resource situations The existing body of work on technology built for disasters and social media use during disasters has extraordinary value, but our work shows substantial gaps left by this field and others: what *other* technologies are people using? What technologies are they *not* using (and why not)? What technologies do they need but not have, if any? We recommend future work branching out to study the diversity of experiences during disasters, including people who are unable or unwilling to use technology, in order to address *all* members of a community. Studying the lack of use of technology is critical to beginning to address systemic inequities caused by misalignments in technical design, disaster response, and social systems.

Through our work, we observed parallels and tensions between disaster preparation/response and security and privacy research, and we strongly recommend security and privacy researchers to follow up on these tensions or alignments in future work. For example, some of the practices we observed (particularly preparations) were at odds with general purpose security and privacy recommendations. Recall, for example, participants' storage sensitive documents in preparation for a storm (Section 5.4.2)—in the cloud, on external hard drives, in email. Though the security community does not tend to agree on specific, prioritized, and actionable advice [245], some might say that users should never store sensitive documents unencrypted in the cloud, or in emails, but these strategies were effective hurricane preparation strategies for some participants. However, there is no technical reason for these practices—document storage safe from technical adversaries and from flooding—to be at odds. This tension, and others like it, are an opportunity for both security and privacy researchers and crisis researchers to consider how their work fits into users lives more holistically.

Additionally, these tensions may actually be an opportunity for the security and privacy community to try the idea of *security and privacy preparedness* as a continual and community-driven process, as natural disaster preparedness is. Das et al. has shown that some cybersecurity behaviors spread socially [71], as our results revealed disaster preparation advice does, so we recommend future work on the idea of security preparedness as a process.

Conclusions Here we have identified two gaps in prior work about technology use during natural disasters: (1) that prior work misses a holistic view of technology use during natural disasters, and (2) that much of the work in the HCI and CSCW communities are focused on technology use, rather than technology disuse. These gaps cause these communities to miss an opportunity to serve marginalized and underprivileged communities, who may have higher barriers to technology use after a natural disaster that affects electrical and connectivity infrastructure. We present a broad view of technology use and disuse during hurricanes in the mainland US, and we offer the broad future research directions to a wide variety of researchers, technologists, and policy makers.

Broader themes about change and vulnerability This chapter differs from the previous 3 in that it focuses on *access* to technology as a necessity for computer security and privacy, but the same themes appear. I explored how hurricanes—a driver of regional change and potential destruction—can limit resources, causing changes in technology use and information needs (theme 1), and how limitations on electricity and connectivity can cause competing needs and uses of technology that leave people unable to fulfill all technology and information needs (theme 2). I also suggest how this prioritization may be cause by system design that does not support low-resource contexts, and that designs that do not support these contexts do a great disservice to communities that have historically experienced systemic disaster aid and infrastructure failures after natural disasters (theme 3). This chapter focuses heavily on how the consequences of failed physical infrastructure interact with technology access, which is a prerequisite for computer security and privacy, and how technical design can potentially *accommodate* physical infrastructure failures, but should not be considered a complete solution, as the issue more broadly stems from infrastructure that is not suited to a warming planet.

Chapter 6

CONCLUSION

Through this dissertation, I have presented case studies of four populations—refugees, Sudanese activists, people considering Covid-19 contact tracing apps, and people who experience hurricanes—undergoing a period of significant change. I have explored three themes, present in each of the four works, that help us understand the relationship between these periods of change and computer security threats and vulnerabilities. Here I revisit these themes, and then suggest broad directions for future work on the idea of designing for change and the nature of vulnerability.

6.1 Summary of themes and work

Chapters 2-5 explored change and vulnerability in four populations; here I summarize the three themes that arise in each chapter about the link between change and vulnerability. I also invite the reader to revisit Table 1.1, which summarizes the presence of each theme in each chapter.

Theme (1): the nature of change itself creates the strong potential for inaccurate and incomplete threat models, which makes people vulnerable to security and privacy harms. Throughout the various types of changes I have investigated, *new* and *modified* threat model elements have been constant: different or changed actors, threats, risks, and technologies. Prior work has found that laypeople have incomplete mental models in general, and may not update them when appropriate [157]; this dissertation explores how a rapidly changing environment contributes to making users' threat models incomplete or inaccurate, which makes them vulnerable to security and privacy harms. Change, thus, makes security and privacy difficult, and it is our responsibility as designers and technologists to support and empower users going through change without expecting that they have a complete threat model.

Refugees, for example, wonder whether they can trust their case managers, or the website that hosts an online job search. Many are also using email and encountering new types of scams for the first time (Chapter 2). Sudanese activists also dealt with changing adversaries (at first the dictator and then the military), unknown adversarial capabilities, and an increased level of risk and threat (Chapter 3). During a hurricane, individuals' needs change, as do their access to resources: hurricanes often damage electrical and connectivity infrastructure, limiting technology use for many in the affected region and leading users to ration technology use. However, hurricanes (and other natural disasters) are also a time of new or increased information needs (Chapter 5). The pandemic also brought new technologies and new risks, and we found that many considered adoption of new technologies (e.g., contact tracing apps) to help offset the new risks of physical interaction, but had incomplete mental models of the risks imposed by the technologies (Chapter 4).

Theme (2): competing needs can change individuals' prioritization of security and privacy. Each change I have explored has surfaced different needs that compete—by design, not by technical necessity—with users' security and privacy. Refugees, for example, experience financial insecurity and may also experience homelessness, health insecurity, and food insecurity; the need to become financially stable drives their technology usage and incentivizes them to prioritize utility over security (Chapter 2). The pandemic also brought financial insecurity for many, along with health risks, and we observed that people weighed security and privacy directly against health when considering whether to use a contact tracing app. Some prioritized security and privacy, while others prioritized health (Chapter 4).

Sudanese activists faced risks to their physical security—as well as digital security—and during the 2018-2019 Sudanese revolution, some prioritized their political goals and fit in security and privacy where possible, despite increased and explicit risks to their safety (Chapter 3). Additionally, during and after hurricanes, we found that people prioritize physical safety and some informatic needs; I explore technology use more broadly than security and privacy, but the changes to technology use (and disuse) show the theme of competing needs changing individuals' use of technology in ways that may create vulnerability (Chapter 5).

Theme (3): Design and advice misalignments increase security and privacy vulnerabilities for groups that are already marginalized by sociopolitical systems and historical inequities. Finally, each chapter in this dissertation has explored some element of sociopolitical vulnerability, and shows that design misalignments exacerbate existing inequalities. My work with refugees surfaces design elements that do not fit many refugees' cultural background: e.g., security questions ask for information that they may not have, the use of birthdays as authenticators works best if all users know their historical birthday, and existing password managers do not account for the power dynamics and information needs between refugees and case managers (Chapter 2). Through my work with activists, I explore another dimension of context—political context. International sanctions and user mental models about the Sudanese government's technical capabilities defined the availability of technology to Sudanese activists during the revolution, showing how design decisions affect users around the world differently due to political boundaries. For example, when Twitter began enforcing two-factor authentication, users could not input a Sudanese phone number and so developed a number of workarounds, such as using a phone number of someone in the Sudanese diaspora, or obtaining an international SIM card (Chapter 3). In Chapter 5, I explore systems- and networking-level technical design misalignments through my work with hurricane survivors: we find that technical design of many apps restricts or entirely prevents users who are experiencing a (in this case, newly) low-resource environment from using technology to accomplish their goals. I also observe that marginalized populations are historically affected most by storms due to systemic disparities in natural disaster aid [91].

Design misalignments are often not insurmountable, but overcoming and working around them imposes extra work on populations that are already bearing the burdens of systemic inequities, or directly increases vulnerability to security and privacy harms.

My work also explores how security advice and user education can be misaligned with the needs and uses of groups who are already marginalized (adding to prior and concurrent work showing similar results, e.g., [196]). Refugees, for example, received advice not to share their social security number or any passwords with anyone, but that advice does not fit their goals and needs, and they were at times left unsure if they were acting securely (Chapter 2). Sudanese activists received advice to use Signal, but were not able to adopt it en masse (Chapter 3). Additionally, we observed systemic gaps in user education about contact tracing apps, as well as prevalent concern about the surveillance of minoritized or vulnerable groups (Chapter 4).

Through these three themes, I capture a deep understanding of the relationship between change and vulnerability, and I have systematically explored how technical design is currently ill-suited to populations experiencing change, creating further vulnerability in already-vulnerable populations.

6.2 What next?

In this dissertation, I have explored why change makes people vulnerable to security and privacy harms, finding that while the nature of change does make people vulnerable, technology often does not support those who are undergoing change, and thus ill-fitted technical designs place further burden on marginalized populations to reach their security and privacy goals. Now, with an understanding of why change and vulnerability are linked, I suggest a few research directions to address a significant question raised by my dissertation: **how do we design for change?**

At a high level, we have to continue to **amplify the voices of vulnerable populations** in our research, to reflect on our motivations for doing such research, and to strive to benefit them at least as much as we benefit ourselves. Specifically, the security and privacy community must continue to learn how to better serve vulnerable and specific populations. Barriers to security, privacy, and safety sometimes overlap between different populations; solutions may benefit multiple populations but can also harm others. Because of this, and because there are *so many* kinds of barriers, we need to continue to do research on and with specific user populations in order to better understand vulnerability and how the needs of different populations both overlap and conflict.

Additionally, something that may be missing from our conception of user research, threat modeling, and *who users are* is, simply, that people's needs, experiences, adversaries, and assets change over time, and when their lives change, they should be supported and empowered by technology as much as they want to be. So, one question for future work is: **how can we bring the idea of *time* and *change* into a threat model, or into our concept of a user?** And, how can we make technologies and user education flexible over time? For many of the users I studied, the kinds of problems that arose from change could have been mitigated with technical designs that actually fit their needs. One solution may be to build in *options* to technical designs in order to empower users to use technology as it fits their situation, with the caveat that too many options can cause user fatigue. For example, instead of thinking about technology for activists when there is an internet blackout, we might think about technology for no-connectivity situations that also works in periods of normal connectivity, specifically as a design that would apply to many users over time (here, activists and people who experience hurricanes). And, can we empower users to choose a different threat model or model of technology use during a period of change?

Finally, there are also users who experience vulnerability due to design misalignments—and these users may be part of marginalized groups—but they may not be experiencing *change*. For example, refugees often experience economic insecurity due to the change of moving to a new country and having little support, but many others groups experience poverty—or political oppression, or low-resource environments, or health risks—without a catalyst. These people are no less important to support and empower.

I suggest exploring other aspects of vulnerability than change, and finding a lens to help us think systematically about how technical design misalignments exacerbate sociopolitical inequities to make users more vulnerable to security, privacy, and safety harms. One concept that may fit is **ontological security**, the security "of being," which encompasses a broad sense of self, safety, and confidence in one's daily routines and relationships [112, 254]. Ontological security may help us think about what other types of security and needs can affect (and be affected by) computer security and privacy—e.g., food security, financial security, health, daily routine, and physical security. For example, future work could ask: how do the social and technical systems that provide assistance those who are food insecure treat security, privacy, safety, and identity? What privacy and security risks does being food insecure impose, if any?

I offer these directions for future work because it is critical for the security and privacy community to better serve marginalized and vulnerable populations—who, in many cases, face high risks and threats to safety and security. In this dissertation, I identify one facet of vulnerability, *change*, and systematically explore how change, security, and privacy intertwine, finding that many technical designs are both ill-suited to the nature of change and mismatched with the needs and uses of users from marginalized groups, exacerbating systemic inequalities during periods of change. I hope that my exploration of change and vulnerability can help researchers, technologists, and policymakers more deeply understand how to design for diverse populations and empower vulnerable populations.

BIBLIOGRAPHY

[1] https://poweroutage.us/area/state/louisiana. [Archived 31-August-2021; accessed 25-March-2022].

[2] eRouška — Part of Smart Quarantine.

[3] Hurricane City. hurricanecity.com. [Accessed 1-June-2021].

[4] Convention and protocol relating to the status of refugees, 1951. http://www.unhcr.org/3b66c2aa10.html.

[5] Refunite. http://refunite.org/, 2017. [Accessed 31-October-2017].

[6] Briefing: Sudanese call for bread and freedom. https://www.thenewhumanitarian.org/news/2019/01/09/Sudan-Bashir-food-protests-bread, January 2019. [Accessed 3-May-2022].

[7] NOAA predicts another active Atlantic hurricane season. https://www.noaa.gov/news-release/noaa-predicts-another-active-atlantic-hurricane-season, May 2021. [Accessed 25-March-2022].

[8] https://www.ready.gov/kit, March 2021. [Accessed 1-April-2021].

[9] Konstantin Aal, Marios Mouratidis, Anne Weibert, and Volker Wulf. Challenges of CI initiatives in a political unstable situation-case study of a computer club in a refugee camp. In *Proceedings of the 19th International Conference on Supporting Group Work*, pages 409–412. ACM, 2016.

[10] Konstantin Aal, George Yerousis, Kai Schubert, Dominik Hornung, Oliver Stickel, and Volker Wulf. Come_in@ Palestine: adapting a German computer club concept to a

Palestinian refugee camp. In *Proceedings of the 5th ACM international conference on Collaboration across boundaries: culture, distance & technology*, pages 111–120. ACM, 2014.

[11] Reem Abbas. How an illegal Sudanese union became the biggest threat to Omar Al Bashir's 29-year reign. `https://www.thenational.ae/world/africa/how-an-illegal-sudanese-union-became-the-biggest-threat-to-omar-al-bashir-s-29-year-reign-1.819159`. [Accessed Sep. 2020].

[12] Reem Abbas. In Sudan, neighbourhoods mobilised against Al-Bashir. `https://www.aljazeera.com/news/2019/05/sudan-neighbourhoods-mobilised-al-bashir-190506182950504.html`. [Accessed Sep. 2020].

[13] Johannes Abeler, Sam Altmann, Luke Milsom, Séverine Toussaert, and Hannah Zillessen. Support in the UK for app-based contact tracing of COVID-19, 2020.

[14] Ruba Abu-Salma, M Angela Sasse, Joseph Bonneau, Anastasia Danilova, Alena Naiakshina, and Matthew Smith. Obstacles to the adoption of secure communication tools. In Úlfar Erlingsson and Bryan Parno, editors, *Proceedings of the 38th IEEE S&P*, pages 137–153. IEEE.

[15] Al Jazeera. Who are Sudan's RSF and their commander Hemeti? `https://www.aljazeera.com/news/2019/06/sudan-rsf-commander-hemeti-190605223433929.html`. [Accessed Sep. 2020].

[16] Khalid Albaih. How WhatsApp is fuelling a 'sharing revolution' in Sudan. `https://www.theguardian.com/world/2015/oct/15/sudan-whatsapp-sharing-revolution`, 10 2015. [Accessed Sep. 2020].

[17] Martin R. Albrecht, Jorge Blasco, Rikke Bjerg Jensen, and Lenka Marekova. Mesh messaging in large-scale protests: Breaking Bridgefy. `https://martinralbrecht.files.wordpress.com/2020/08/bridgefy-abridged.pdf`. [Accessed 9-2020].

[18] Ali Alkhatib. We need to talk about digital contact tracing. https://ali-alkhatib.com/blog/digital-contact-tracing, May 2020. [Accessed 6-May-2020].

[19] Asam Almohamed and Dhaval Vyas. Vulnerability of displacement: Challenges for integrating refugees and asylum seekers in host communities. In *Proceedings of the 28th Australian Conference on Computer-Human Interaction*, pages 125–134. ACM, 2016.

[20] Samuel Altmann, Luke Milsom, Hannah Zillessen, Raffaele Blasone, Frederic Gerdon, Ruben Bach, Frauke Kreuter, Daniele Nosenzo, Severine Toussaert, and Johannes Abeler. Acceptability of app-based contact tracing for COVID-19: Cross-country survey evidence. *Available at SSRN 3590505*, 2020.

[21] Amnesty International Org. Agents of fear: the National Security Service in Sudan. https://www.amnesty.org/download/Documents/36000/afr540102010en.pdf. [Accessed Sep. 2020].

[22] Amnesty International Org. Sudan: All security agencies that attacked protesters must be held to account. https://www.amnesty.org/en/latest/news/2020/03/sudan-all-security-agencies-that-attacked-protesters-must-be-held-to-account/. [Accessed Sep. 2020].

[23] Monica Anderson and Brooke Auxier. Most Americans don’t think cellphone tracking will help limit COVID-19, are divided on whether it’s acceptable. *Pew Research Center*, April 2020.

[24] Apple Inc. Use screen time on your iPhone, iPad, or iPod touch. https://support.apple.com/en-us/HT208982. [Accessed Sep. 2020].

[25] Sandra Appleby-Arnold, Noellie Brockdorff, Laure Fallou, and Rémy Bossu. Truth, trust, and civic duty: Cultural factors in citizens’ perceptions of mobile phone apps and

social media in disasters. *Journal of contingencies and crisis management*, 27(4):293–305, 2019.

[26] Leah Asmelash and Saeed Ahmed. Everything you need to know to prepare for a natural disaster. `https://www.cnn.com/2019/07/12/us/how-to-prepare-for-natural-disasters-trnd`, July 2019. [Accessed 1-April-2021].

[27] ASUS Inc. ZenFone what is Twin Apps and how does it work? `https://www.asus.com/support/FAQ/1032388/`. [Accessed Sep. 2020].

[28] BeAware Bahrain. `https://play.google.com/store/apps/details?id=bh.bahrain.corona.tracker&hl=en_US`.

[29] Jennifer Baranoff, R Israel Gonzales, Jay Liu, Heidi Yang, and Jimin Zheng. Lantern: Empowering refugees through community-generated guidance using near field communication. In *Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems*, pages 7–12. ACM, 2015.

[30] BBC. Coronavirus: Austria locks down as new wave grips Europe. `https://www.bbc.com/news/world-europe-54945400`. [Accessed 14-November-2020].

[31] BBC News. Egypt's Muslim Brotherhood declared 'terrorist group'. `https://www.bbc.com/news/world-middle-east-25515932`. [Accessed Sep. 2020].

[32] Steven Bellman, Eric J Johnson, Stephen J Kobrin, and Gerald L Lohse. International differences in information privacy concerns: A global survey of consumers. *The Information Society*, 20(5):313–324, 2004. Taylor & Francis.

[33] Ruha Benjamin. Race after technology: Abolitionist tools for the new jim code. *Social forces*, 2019.

[34] Eric S Blake, Chris Landsea, and Ethan J Gibney. The deadliest, costliest, and most intense united states tropical cyclones from 1851 to 2010 (and other frequently requested hurricane facts). 2011.

[35] Matthew Bloch, Charlie Smart, Jesse McKinley, Nate Schweber, Amanda Rosa, Chelsia Rose Marcius, Jon Hurdle, and Campbell Robertson. Flooding from Ida kills dozens of people in four states. https://web.archive.org/web/20210905084322/https://www.nytimes.com/live/2021/09/02/nyregion/nyc-storm, September 2021. Archived Sept 3 2021; accessed March 25 2022.

[36] Stevens Le Blond, Adina Uritesc, Cédric Gilbert, Zheng Leong Chua, Prateek Saxena, and Engin Kirda. A look at targeted attacks through the lense of an NGO. In *23rd USENIX Security Symposium*, 2014.

[37] Morgan Marquis Boire, Jakub Dalek, Sarah McKune, Matthew Carrieri, Masashi Crete-Nishihata, Ron Deibert, Saad Omar Khan, John Scott-Railton, and Greg Wiseman. Planet Blue Coat: Mapping global censorship and surveillance tools. https://citizenlab.ca/wp-content/uploads/2015/03/Planet-Blue-Coat-Mapping-Global-Censorship-and-Surveillance-ToolsPlanet-Blue-Coat-Mapping-Global-Censorship-and-Surveillance-Tools.pdf, 1 2013. [Accessed Dec. 2020].

[38] Norman M Bradburn, Lance J Rips, and Steven K Shevell. Answering autobiographical questions: The impact of memory and inference on surveys. *Science*, 236(4798):157–161, 1987.

[39] Alina Bradford. 18 tips to prepare for a natural disaster. https://www.cnet.com/pictures/prepare-for-a-natural-disaster-with-these-tips-wildfire-flood-hurricane-tornado/, October 2019. [Accessed 1-April-2021].

[40] Deana Brown and Rebecca E Grinter. Designing for transient use: A human-in-the-

loop translation platform for refugees. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, pages 321–330. ACM, 2016.

[41] Dave Burke. An update on exposure notifications. `https://blog.google/inside-google/company-announcements/update-exposure-notifications/`. [Accessed 14-November-2020].

[42] Karoline Busse, Julia Schäfer, and Matthew Smith. Replication: No one can hack my mind revisiting a study on expert and non-expert security practices and advice. In *Proceedings of the 15th SOUPS*. USENIX.

[43] Justin Chan, Dean Foster, Shyam Gollakota, Eric Horvitz, Joseph Jaeger, Sham Kakade, Tadayoshi Kohno, John Langford, Jonathan Larson, Sudheesh Singanamalla, Jacob Sunshine, and Stefano Tessaro. PACT: Privacy-sensitive protocols and mechanisms for mobile contact tracing, 2020.

[44] Nick Charalambides. We recently went viral on TikTok - here's what we learned. `https://blog.prolific.co/we-recently-went-viral-on-tiktok-heres-what-we-learned/`, August 2021. [Accessed 6-September-2021].

[45] Kathy Charmaz. *Constructing Grounded Theory.* SAGE Publications Ltd, second edition, 2014.

[46] Reuters Fact Check. Fact check—Zello 'walkie-talkie' natural disaster app requires internet access. `https://www.reuters.com/article/factcheck-zello-walkie/fact-check-zello-walkie-talkie-natural-disaster-app-requires-internet-access-idUSL1N2Q31SN`, September 2021. Accessed April 11 2022.

[47] Christine Chen, Nicola Dell, and Franziska Roesner. Computer security and privacy in the interactions between victim service providers and human trafficking survivors. In *28th {USENIX} Security Symposium ({USENIX} Security 19)*, pages 89–104, 2019.

[48] France Cheong and Christopher Cheong. Social media data mining: A social network analysis of tweets during the 2010-2011 Australian floods. *PACIS*, 11:46–46, 2011.

[49] Jan Wesner Childs. Hurricane Ida: Roads flooded, buildings ripped apart, hundreds of thousands without power in Louisiana. `https://web.archive.org/web/20210829235352/https://weather.com/news/news/2021-08-29-hurricane-ida-louisiana-new-orleans-mississippi-news`, August 2021. [Archived 29-August-2021; accessed 25-March-2022].

[50] Hichang Cho, Milagros Rivera-Sánchez, and Sun Sun Lim. A multinational study on online privacy: Global concerns and local responses. *New Media & Society*, 11(3):395–416, 2009. SAGE.

[51] Clara Chong. About 1 million people have downloaded TraceTogether app, but more need to do so for it to be effective: Lawrence Wong. *The Straits Times*, April 2020. [Accessed 24-April-2020].

[52] Richard Clayton, Steven J Murdoch, and Robert NM Watson. Ignoring the great firewall of China. In *International Workshop on Privacy Enhancing Technologies*, pages 20–35. Springer, 2006.

[53] Juli Clover. Apple's exposure notification system: Everything you need to know. `https://www.macrumors.com/guide/exposure-notification/`, September 2020. [Accessed 14-November-2020].

[54] Camille Cobb, Ted McCarthy, Annuska Perkins, Ankitha Bharadwaj, Jared Comis, Brian Do, and Kate Starbird. Designing for the deluge: understanding & supporting the distributed, collaborative work of crisis volunteers. In *Proceedings of the 17th ACM conference on Computer supported cooperative work & social computing*, pages 888–899, 2014.

[55] D'vera Cohn. Census considers new approach to asking about race – by not using the term at all, 2015.

[56] MinSalud Digital. `https://play.google.com/store/apps/details?id=co.gov.ins.guardianes&hl=en_US`.

[57] European Commission. COVID-19 media surveillance — 31 March 2020. `https://ec.europa.eu/jrc/en/science-update/covid-19-media-surveillance-20200331`. [Accessed 22-April-2020].

[58] European Commission. COVID-19 media surveillance — 1 April 2020. `https://ec.europa.eu/jrc/en/science-update/covid-19-media-surveillance-20200401`, April 2020. [Accessed 23-April-2020].

[59] Sunny Consolvo, Katherine Everitt, Ian Smith, and James A Landay. Design requirements for technologies that encourage physical activity. In Gary Olson, editor, *Proceedings of the 2006 ACM SIGCHI CHI*, pages 457–466. ACM.

[60] Juliet Corbin and Anselm Strauss. *Basics of qualitative research.* Sage publications, 2015.

[61] Coronamap. `https://coronamap.site/`.

[62] Jedidiah R. Crandall, Earl Barr, Daniel Zinn, Rich East, and Michael Byrd. Conceptdoppler: A weather tracker for internet censorship. In Peng Ning, Sabrina De Capitani di Vimercati, and Paul F. Syverson, editors, *Proceedings of the 14th ACM SIGSAC CCS*, pages 352–365. ACM.

[63] Andrew Crocker, Kurt Opsahl, and Bennett Cyphers. The challenge of proximity apps for COVID-19 contact tracing. `https://www.eff.org/deeplinks/2020/04/challenge-proximity-apps-covid-19-contact-tracing`, April 2020.

[64] Mark É Czeisler, Michael A Tynan, Mark E Howard, Sally Honeycutt, Erika B Fulmer, Daniel P Kidder, Rebecca Robbins, Laura K Barger, Elise R Facer-Childs, Grant Baldwin, et al. Public attitudes, behaviors, and beliefs related to covid-19, stay-at-home orders, nonessential business closures, and public health guidance—United States, New York City, and Los Angeles, May 5–12, 2020. *Morbidity and Mortality Weekly Report*, 69(24):751, 2020.

[65] Dabanga Radio. Google apps available in Sudan as US eases sanctions. `https://www.dabangasudan.org/en/all-news/article/google-apps-available-in-sudan-as-us-eases-sanctions`, 7 2015. [Accessed Aug. 2020].

[66] Alaa Daffalla, Lucy Simko, Tadayoshi Kohno, and Alexandru G. Bardas. Defensive technology use by political activists during the sudanese revolution. In *2021 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2021.

[67] Negin Dahya and Sarah Dryden-Peterson. Tracing pathways to higher education for refugees: the role of virtual support networks and mobile phones for women in refugee camps. *Comparative Education*, 53(2):284–301, 2017.

[68] Dharma Dailey and Kate Starbird. Visible skepticism: Community vetting after Hurricane Irene. In *ISCRAM*, 2014.

[69] Alberto Dainotti, Claudio Squarcella, Emile Aben, Kimberly C Claffy, Marco Chiesa, Michele Russo, and Antonio Pescapé. Analysis of country-wide internet outages caused by censorship. In Patrick Thiran and Walter Willinger, editors, *Proceedings of the 11th Internet Measurement Conference (IMC)*, pages 1–18. ACM.

[70] Sauvik Das, Laura A Dabbish, and Jason I Hong. A typology of perceived triggers for end-user security and privacy behaviors. In Michelle Mazurek and Rob Reeder, editors, *Proceedings of the 15th SOUPS*, Santa Clara, CA, USA. USENIX.

[71] Sauvik Das, Adam DI Kramer, Laura A Dabbish, and Jason I Hong. The role of social influence in security feature adoption. In Dan Cosley, Andrea Forte, Luigina Ciolfi, and David McDonald, editors, *Proceedings of the 18th ACM SIGCHI CSCW*, pages 1416–1426. ACM.

[72] Alejandro de la Garza. Contact tracing apps were big tech's best idea for fighting COVID-19. Why haven't they helped? https://time.com/5905772/covid-19-contact-tracing-apps/. [Accessed 13-November-2020].

[73] Rianne Dekker, Godfried Engbersen, Jeanine Klaver, and Hanna Vonk. Smart refugees: How Syrian asylum migrants use social media information in migration decision-making. *Social Media+ Society*, 4(1):2056305118764439, 2018.

[74] Nicola Dell, Vidya Vaidyanathan, Indrani Medhi, Edward Cutrell, and William Thies. "Yours is better!" Participant response bias in HCI. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 1321–1330, 2012.

[75] Simon Dennis, Paul Garrett, Joshua White, Daniel Little, Amy Perfors, Yoshihisa Kashima, and Stephan Lewandowsky. A representative sample of Australian participant's attitudes towards government tracking during the COVID-19 pandemic. https://paulgarrettphd.github.io/Site/Wave2Final.html, 4 2020. [Accessed 21-October-2020].

[76] Simon Dennis, Stephan Lewandowsky, Philipp Lorenz-Spreen, Klaus Oberauer, Yasmina Okan, Rob Goldstone, Yang Cheng-Ta, Yoshihisa Kashima, Amy Perfors, Josh White, Paul Garrett, Nic Geard, Daniel Little, Lewis Mitchell, Martin Tomko, Anastasia Kozyreva, Stefan Herzog, Ralph Hertwig, Thorsten Pachur, Muhsin Yesilada, and Marcus Butavicius. Social licensing of privacy-encroaching policies to address the COVID-19 pandemic. https://stephanlewandowsky.github.io/UKsocialLicence/index.html. [Accessed 19-October-2020].

[77] Claudia Der-Martirosian, Leonie Heyworth, Karen Chu, Yvonne Mudoh, and Aram Dobalian. Patient characteristics of va telehealth users during hurricane harvey. *Journal of Primary Care & Community Health*, 11:2150132720931715, 2020.

[78] Alexander Dhoest. Digital (dis) connectivity in fraught contexts: The case of gay refugees in Belgium. *European Journal of Cultural Studies*, 23(5):784–800, 2020.

[79] Jill Patrice Dimond. *Feminist HCI for real: Designing technology in support of a social movement*. PhD thesis, Georgia Institute of Technology, 2012.

[80] Zak Doffman. Forget Apple and Google—here's the real challenge for COVID-19 contact-tracing. `https://www.forbes.com/sites/zakdoffman/2020/04/12/forget-apple-and-google-heres-the-real-challenge-for-covid-19-contact-tracing/\#4f9426092709`, April 2020. [Accessed 21-April-2020].

[81] Sarah Dryden-Peterson, Negin Dahya, and Dacia Douhaibi. How teachers use mobile phones as education tools in refugee camps, March 2017.

[82] Tristan Endsley, Yu Wu, James Reep, J Eep, and J Reep. The source of the story: Evaluating the credibility of crisis information sources. In *ISCRAM*, 2014.

[83] Darrell Etherington. Apple launches COVID-19 "exposure notification express" with iOS 13.7 — Android to follow later this month. `https://techcrunch.com/2020/09/01/apple-launches-system-level-covid-19-exposure-notification-express-with-ios-13-7-google-to-follow-later-this-month/`, September 2020. [Accessed 14-November-2020].

[84] European Council on Foreign Relations. Bad company: How dark money threatens Sudan's transition. `https://www.ecfr.eu/publications/summary/bad_company_how_dark_money_threatens_sudans_transition`. [Accessed Sep. 2020].

[85] Evaluate: Covid-19 daily update. `https://www.evaluate.com/covid-19-daily-update`.

[86] Lilla Farkas. Data collection in the field of ethnicity: Analysis and comparative review of equality data collection practices in the European Union.

[87] Luca Ferretti, Chris Wymant, Michelle Kendall, Lele Zhao, Anel Nurtay, Lucie Abeler-Dörner, Michael Parker, David Bonsall, and Christophe Fraser. Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. *Science*, 2020.

[88] Thomas Ferris, Erick Moreno-Centeno, Justin Yates, Kisuk Sung, Mahmoud El-Sherif, and David Matarrita-Cascante. Studying the usage of social media and mobile technology during extreme events and their implications for evacuation decisions: A case study of Hurricane Sandy. *International Journal of Mass Emergencies & Disasters*, 34(2), 2016.

[89] Casey Fiesler, Shannon Morrison, and Amy S Bruckman. An archive of their own: A case study of feminist HCI and values in design. In *Proceedings of the 2016 ACM SIGCHI CHI*, pages 2574–2585. ACM.

[90] Joshua Filer and Daniel Gheorghiu. Test, track, and trace: How is the NHSX covid app performing in a hospital setting? *medRxiv*, 2020.

[91] Megan Finn. *Documenting Aftermath: Information Infrastructures in the Wake of Disasters*. Massachussetts Institute of Technology, 2018.

[92] Jennifer Flemming. Making online connections. October 2011.

[93] Elizabeth Flock. Syria internet services shut down as protesters fill streets. `https://www.washingtonpost.com/blogs/blogpost/post/syria-internet-services-shut-down-as-protesters-fill-streets/2011/06/03/AGtLwxHH_blog.html`. [Accessed Sep. 2020].

[94] US Food, Drug Administration, et al. Collection of race and ethnicity data in clinical trials: Guidance for industry and food and drug administration staff. *Rockville, MD: US Food and Drug Administration*, 2016.

[95] U.S. Committee for Refugees and Immigrants. Refugee resettlement. `http://refugees.org/explore-the-issues/our-work-with-refugees/refugeeresettlementprocess/`, 2017. [Accessed 29-October-2017].

[96] United Nations High Commissioner for Refugees (UNHCR). Global trends: Forced displacement in 2016. `http://www.unhcr.org/globaltrends2016/`, 2017. [Accessed 19-October-2017].

[97] United Nations High Commissioner for Refugees (UNHCR). Resettlement in the United States. `http://www.unhcr.org/en-us/resettlement-in-the-united-states.html`, 2017. [Accessed 28-October-2017].

[98] Karen Freberg, Kristin Saling, Kathleen G Vidoloff, and Gina Eosco. Using value modeling to evaluate social media messages: The case of Hurricane Irene. *Public Relations Review*, 39(3):185–192, 2013.

[99] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levyand Thomas Ristenpart, and Nicola Dell. Digital technologies and intimate partner violence: A qualitative analysis with multiple stakeholders. In *PACM: Human-Computer Interaction: Computer-Supported Cooperative Work and Social Computing (CSCW)*, 2017.

[100] JC Gaillard. Power, prestige & forgotten values: A disaster studies manifesto. `https://www.ipetitions.com/petition/power-prestige-forgotten-values-a-disaster`. [Accessed 24-April-2022].

[101] JC Gaillard and Lori Peek. Disaster-zone research needs a code of conduct, 2019.

[102] Paul Garrett, Joshua Paul White, Stephan Lewandowsky, Yoshihisa Kashima, Andrew Perfors, Daniel R Little, Nic Geard, Lewis Mitchell, Martin Tomko, and Simon Dennis. The acceptability and uptake of smartphone tracking for COVID-19 in Australia. 2020.

[103] Scott Garriss, Rámon Cáceres, Stefan Berger, Reiner Sailer, Leendert van Doorn, and Xiaolan Zhang. Trustworthy and personalized computing on public kiosks. In *6th International Conference on Mobile Systems, Applications, and Services (MobiSys)*, 2008.

[104] Alexey Gavrilov. How to use Zello for communication during a disaster. `https://blog.zello.com/how-to-use-zello-during-an-emergency`, August 2019. [Accessed 11-April-2022].

[105] Shirley Gaw, Edward W Felten, and Patricia Fernandez-Kelly. Secrecy, flagging, and paranoia: Adoption criteria in encrypted email. In *Proceedings of the 2006 ACM SIGCHI CHI*, pages 591–600. ACM.

[106] Genevieve Gebhart and Tadayoshi Kohno. Internet censorship in Thailand: User practices and potential threats. In Andrei Sabelfeld and Matthew Smith, editors, *Proceedings of the 2nd IEEE EuroS&P*, pages 417–432. IEEE.

[107] Christine Geeng and Alexis Hiniker. LGBTQ privacy concerns on social media. In *CHI 2018 Workshop Exploring Individual Differences in Privacy*, 2018.

[108] Christine Geeng, Savanna Yee, and Franziska Roesner. Fake news on Facebook and Twitter: Investigating how people (don't) investigate. In Regina Bernhaupt, Florian Mueller, and Josh Andres, editors, *Proceedings of the 2020 ACM SIGCHI CHI*, pages 1–14. ACM.

[109] Jacob Gershman. A guide to state coronavirus lockdowns. *The Wall Street Journal*, March 2020.

[110] Samuel Getachew. The internet is back on in Ethiopia but there's every chance it'll be off again soon. https://qz.com/africa/1884387/ethiopia-internet-is-back-on-but-oromo-tensions-remain/, 7 2020. [Accessed Aug. 2020].

[111] GH Covid-19. http://ghcovid19.com/.

[112] Anthony Giddens. Ontological security and existential anxiety. In *Modernity and self-identity: Self and society in the late modern age*, pages 35–69. Stanford University Press, 1991.

[113] Phillipa Gill, Masashi Crete-Nishihata, Jakub Dalek, Sharon Goldberg, Adam Senft, and Greg Wiseman. Characterizing web censorship worldwide: Another look at the opennet initiative data. *Transactions on the Web (TWEB)*, 9(1):1–29, 2015. ACM.

[114] Marie Gillespie, Lawrence Ampofo, Margaret Cheesman, Becky Faith, Evgenia Iliadou, Ali Issa, Souad Osseiran, and Dimitris Skleparis. Mapping refugee media journeys: Smartphones and social media networks. 2016.

[115] James D Goltz and Dennis S Mileti. Public response to a catastrophic southern california earthquake: A sociological perspective. *Earthquake spectra*, 27(2):487–504, 2011.

[116] Dan Goodin. Chinese bank requires foreign firm to install app with covert backdoor. https://arstechnica.com/information-technology/2020/06/chinese-bank-requires-foreign-firm-to-install-app-with-covert-backdoor/, 6 2020. [Accessed Sep. 2020].

[117] Google. Apple and Google partner on COVID-19 contact tracing technology. https://web.archive.org/web/20200410202023/https://www.blog.google/inside-google/company-announcements/apple-and-google-partner-covid-19-contact-tracing-technology/, April 2020. [Accessed 10-April-2020].

[118] Google LLC. Supported locations for distribution to Google Play users. https://support.google.com/googleplay/android-developer/table/3541286?hl=en. [Accessed Sep. 2020].

[119] Andrea Grimes and Rebecca E Grinter. Designing persuasion: Health technology for low-income African American communities. In *Proc. International Conference on Persuasive Technology*, pages 24–35. Springer, 2007.

[120] Matthew Guariglia and Adam Schwartz. Protecting civil liberties during a public health crisis. https://www.eff.org/deeplinks/2020/03/protecting-civil-liberties-during-public-health-crisis, March 2020.

[121] Tamy Guberek, Allison McDonald, Sylvia Simioni, Abraham H Mhaidli, Kentaro Toyama, and Florian Schaub. Keeping a low profile? Technology, risk and privacy among undocumented immigrants. In Regan L. Mandryk, Mark Hancock, Mark Perry, and Anna L. Cox, editors, *Proceedings of the 2018 ACM SIGCHI CHI*, pages 1–15. ACM.

[122] G. Guest, A. Bunce, and L. Johnson. How many interviews are enough? An experiment with data saturation and variability. *Field Methods*, 18(1), 2006.

[123] M Guillon and P Kergall. Attitudes and opinions on quarantine and support for a contact-tracing application in France during the COVID-19 outbreak. *Public health*, 188:21–31, 2020.

[124] Aditi Gupta, Hemank Lamba, Ponnurangam Kumaraguru, and Anupam Joshi. Faking Sandy: Characterizing and identifying fake images on Twitter during Hurricane Sandy. In *Proceedings of the 22nd international conference on World Wide Web*, pages 729–736, 2013.

[125] Emily Guskin. Hurricane Sandy and Twitter. https://www.pewresearch.org/

journalism/2012/11/06/hurricane-sandy-and-twitter/, 11 2012. [Accessed April 21 2022.

[126] Steffen Haesler, Ragnar Mogk, Florentin Putz, Kevin T Logan, Nadja Thiessen, Katharina Kleinschnitger, Lars Baumgärtner, Jan-Philipp Stroscher, Christian Reuter, Michèle Knodt, et al. Connected self-organized citizens in crises: An interdisciplinary resilience concept for neighborhoods. In *Companion Publication of the 2021 Conference on Computer Supported Cooperative Work and Social Computing*, pages 62–66, 2021.

[127] David M. Halbfinger, Isabel Kershner, and Ronen Bergman. To track coronavirus, Israel moves to tap secret trove of cellphone data. *The New York Times*, March 2020. [Accessed 29-March-2020].

[128] Arianna Hanchey, Amy Schnall, Tesfaye Bayleyegn, Sumera Jiva, Anna Khan, Vivi Siegel, Renée Funk, and Erik Svendsen. Notes from the field: Deaths related to Hurricane Ida reported by media—Nine states, August 29–September 9, 2021.

[129] Marian Harbach, Alexander De Luca, Nathan Malkin, and Serge Egelman. Keep on lockin' in the free world: A multi-national comparison of smartphone locking. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, pages 4823–4827, 2016.

[130] Seth Hardy, Masashi Crete-Nishihata, Katharine Kleemola, Adam Senft, Byron Sonne, Greg Wiseman, Phillipa Gill, and Ronald J. Deibert. Targeted threat index: Characterizing and quantifying politically-motivated targeted malware. In *23rd USENIX Security Symposium*, 2014.

[131] Eszter Hargittai and Elissa Redmiles. Covid-19 study on digital media and the coronavirus pandemic. http://webuse.org/covid/. [accessed on Nov 17 2020].

[132] Eszter Hargittai and Elissa Redmiles. Will Americans be willing to install COVID-19 tracking apps? *Scientific American*, April 2020.

[133] Mai Hassan and Ahmed Kodouda. Sudan's uprising: The fall of a dictator. *The Journal of Democracy*, 30(4):89–103, 10 2019. Johns Hopkins University Press.

[134] Joel Hellewell, Sam Abbott, Amy Gimma, Nikos I Bosse, Christopher I Jarvis, Timothy W Russell, James D Munday, Adam J Kucharski, W John Edmunds, Fiona Sun, et al. Feasibility of controlling COVID-19 outbreaks by isolation of cases and contacts. *The Lancet Global Health*, 2020.

[135] Edward A Hirsch. *Contestational design: Innovation for political activism.* PhD thesis, MIT, 2008.

[136] Tad Hirsch. Feature learning from activists: Lessons for designers. *Interactions*, 16(3):31–33, 2009. ACM.

[137] Tad Hirsch and John Henry. TXTmob: Text messaging for protest swarms. In *ACM SIGCHI CHI*, pages 1455–1458. ACM. Abstract.

[138] Philip N Howard, Aiden Duffy, Deen Freelon, Muzammil M Hussain, Will Mari, and Marwa Maziad. Opening closed regimes: What was the role of social media during the Arab Spring? *Available at SSRN 2595096*, 2011.

[139] Kendall Howell. The fifth amendment, decryption and biometric passcodes. `https://www.lawfareblog.com/fifth-amendment-decryption-and-biometric-passcodes`, 11 2017. [Accessed Aug. 2020].

[140] Jeremy Hsu. How India, the world's largest democracy, shuts down the internet. `https://spectrum.ieee.org/tech-talk/telecom/internet/how-the-worlds-largest-democracy-shuts-down-the-internet`, 1 2020. [Accessed Aug. 2020].

[141] Amanda L Hughes, Lise AA St. Denis, Leysia Palen, and Kenneth M Anderson. Online public communications by police & fire services during the 2012 Hurricane Sandy. In *Proceedings of the SIGCHI conference on human factors in computing systems*, pages 1505–1514, 2014.

[142] Amanda Lee Hughes and Leysia Palen. Twitter adoption and use in mass convergence and emergency events. *International journal of emergency management*, 6(3-4):248–260, 2009.

[143] Mary Hui. How Taiwan is tracking 55,000 people under home quarantine in real time. *Quartz*, March 2020. [Accessed 26-April-2020].

[144] Human Rights Watch Org. Sudan. `https://www.hrw.org/africa/sudan`. [Accessed Sep. 2020].

[145] Human Rights Watch Org. Sudan: End censorship and repression. `https://www.hrw.org/news/2009/02/18/sudan-end-censorship-and-repression`. [Accessed Sep. 2020].

[146] Muhammad Ikram, Narseo Vallina-Rodriguez, Suranga Seneviratne, Mohamed Ali Kaafar, and Vern Paxson. An analysis of the privacy and security risks of Android VPN permission-enabled apps. In Phillipa Gill and John Heidemann, editors, *Proceedings of the 16th Internet Measurement Conference (IMC)*, pages 349–364. ACM.

[147] Mary Ilyushina. How Russia is using authoritarian tech to curb coronavirus. *CNN*, March 2020.

[148] Aarogya Setu. `https://play.google.com/store/apps/details?id=nic.goi.aarogyasetu&hl=en_US`.

[149] Inria. `https://github.com/ROBERT-proximity-tracing/documents`.

[150] Iulia Ion, Rob Reeder, and Sunny Consolvo. “... no one can hack my mind”: Comparing expert and non-expert security practices. In Lorrie Faith Cranor, Robert Biddle, and Sunny Consolvo, editors, *Proceedings of the 11th SOUPS*. USENIX.

[151] Hamagen. `https://play.google.com/store/apps/details?id=com.hamagen&hl=en_US`.

[152] Stephanie Maria Jansen-Kosterink, Marian Hurmuz, Marjolein den Ouden, and Lex van Velsen. Predictors to use mobile apps for monitoring COVID-19 symptoms and contact tracing: A survey among Dutch citizens. *medRxiv*, 2020.

[153] Jessica Jones. Spain toughens restrictions as coronavirus death toll surges. *Reuters*, March 2020. [Accessed 22-April-2020].

[154] Mark Jurkowitz, Amy Mitchell, Elisa Shearer, and Mason Walker. U.S. media polarization and the 2020 election: A nation divided. `https://www.pewresearch.org/journalism/2020/01/24/u-s-media-polarization-and-the-2020-election-a-nation-divided/`, January 2020.

[155] Rafi Kabarriti, N Patrik Brodin, Maxim I Maron, Chandan Guha, Shalom Kalnicki, Madhur K Garg, and Andrew D Racine. Association of race and ethnicity with comorbidities and survival among patients with COVID-19 at an urban medical center in New York. *JAMA network open*, 3(9):e2019795–e2019795, 2020.

[156] Ruogu Kang, Stephanie Brown, Laura Dabbish, and Sara Kiesler. Privacy attitudes of Mechanical Turk workers and the US public. In *Symposium on Usable Privacy and Security (SOUPS)*, volume 4, page 1, 2014.

[157] Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. “My data just goes everywhere:” User mental models of the internet and implications for privacy and security. In *Eleventh Symposium on Usable Privacy and Security (SOUPS 2015)*, pages 39–52, 2015.

[158] Neeta Kantamneni. The impact of the covid-19 pandemic on marginalized populations in the united states: A research agenda. *Journal of vocational behavior*, 119:103439, 2020.

[159] Gabriel Kaptchuk, Daniel Goldstein, Eszter Hargittai, Jake M Hofman, and Elissa M Redmiles. How good is good enough? quantifying the impact of benefits, accuracy, and privacy on willingness to adopt covid-19 decision aids. *Digital Threats: Research and Practice*.

[160] Sophie Kasakove. Three weeks after Hurricane Ida, parts of southeast Louisiana are still dark. `https://www.nytimes.com/2021/09/18/us/ida-louisiana-power-outages.html`, September 2021. [Accessed 25-March-2022].

[161] Jennifer Kates, Josh Michaud, and Jennifer Tolbert. Stay-at-home orders to fight COVID-19 in the United States: The risks of a scattershot approach. *KFF*, April 2020.

[162] Jamey Keaten and Frank Jordans. More masks, less play: Europe tightens rules as virus surges, October 2020. [Accessed 14-November-2020].

[163] Simon Kemp. Digital 2018: Sudan. `https://datareportal.com/reports/digital-2018-sudan?rq=sudan`. [Accessed Aug. 2020].

[164] Max S. Kim. South Korea is watching quarantined citizens with a smartphone app. `https://www.technologyreview.com/2020/03/06/905459/coronavirus-south-korea-smartphone-app-quarantine/`, 3 2020. [Accessed 19-November-2020].

[165] Min Joo Kim and Simon Denyer. A 'travel log' of the times in South Korea: Mapping the movements of coronavirus carriers. *The Washington Post*, March 2020. [Accessed 26-April-2020].

[166] Nemo Kim. 'More scary than coronavirus': South Korea's health alerts expose private lives. *The Guardian*, March 2020.

[167] Patrick Kingsley. *The new odyssey: The story of Europe's refugee crisis.* Guardian Faber Publishing, 2016.

[168] Sarah Knapton. How long will the UK coronavirus lockdown last? *Telegraph*, April 2020. [Accessed 27-April-2020].

[169] Rakesh Kochhar. Unemployment rose higher in three months of COVID-19 than it did in two years of the great recession. `https://www.pewresearch.org/fact-tank/2020/06/11/unemployment-rose-higher-in-three-months-of-covid-19-than-it-did-in-two-years-of-the-great-recession/`, June 2020. [Accessed 5-May-2022].

[170] Marina Kogan, Leysia Palen, and Kenneth M Anderson. Think local, retweet global: Retweeting by the geographically-vulnerable during Hurricane Sandy. In *Proceedings of the 18th ACM conference on computer supported cooperative work & social computing*, pages 981–993, 2015.

[171] Genia Kostka and Sabrina Habich-Sobiegalla. In times of crisis: Public perceptions towards COVID-19 contact tracing apps in China, Germany and the US. *Germany and the US (September 16, 2020)*, 2020.

[172] Andrew E. Kramer. Ukraine's opposition says government stirs violence. `https://www.nytimes.com/2014/01/22/world/europe/ukraine-protests.html`, 1 2014. [Accessed Sep. 2020].

[173] Stephanie Kramer. More Americans say they are regularly wearing masks in stores and other businesses. `https://www.pewresearch.org/fact-tank/2020/08/27/more-americans-say-they-are-regularly-wearing-masks-in-stores-and-other-businesses/`, August 2020.

[174] Jens Manuel Krogstad. Key facts about refugees to the U.S. `https:`

//www.pewresearch.org/fact-tank/2019/10/07/key-facts-about-refugees-to-the-u-s/, October 2010. [Accessed 2-May-2022].

[175] Susan Landau, Christy E. Lopez, and Laura Moy. The importance of equity in contact tracing. https://www.lawfareblog.com/importance-equity-contact-tracing, May 2020.

[176] Mark Latonero and Irina Shklovski. Emergency management, Twitter, and social media evangelism. *International Journal of Information Systems for Crisis Response and Management (IJISCRAM)*, 3(4):1–16, 2011.

[177] Andy S Latto and Robbie Berg. National hurricane center tropical cyclone report: Hurricane Nicholas, March 2022.

[178] Alex Ledsom. New EU travel restrictions, country by country, as Europe locks down. https://www.forbes.com/sites/alexledsom/2020/11/12/new-eu-travel-bans-country-by-country-covid-19-restrictions-as-europe-locks-down/?sh=34b75c466f80, November 2020. [Accessed 14-November-2020].

[179] Linda Leung. Telecommunications across borders: Refugees' technology use during displacement. *Telecommunications Journal of Australia*, 2010.

[180] Jessica Li and H Raghav Rao. Twitter as a rapid response news service: An exploration in the context of the 2008 China earthquake. *The Electronic Journal of Information Systems in Developing Countries*, 42(1):1–22, 2010.

[181] Tianshi Li, Cori Faklaris, Jennifer King, Yuvraj Agarwal, Laura Dabbish, Jason I Hong, et al. Decentralized is not risk-free: Understanding public perceptions of privacy-utility trade-offs in COVID-19 contact-tracing apps. *arXiv preprint arXiv:2005.11957*, 2020.

[182] Xuyang Li, Antara Bahursettiwar, and Marina Kogan. Hello? Is there anybody in there? Analysis of factors promoting response from authoritative sources in crisis. *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW1):1–21, 2021.

[183] Amy Livingston. How to get emergency financial assistance & help with bills —- Resources. https://www.moneycrashers.com/prepare-natural-disaster-emergency-preparedness/, December 2021. [Accessed 1-April-2021].

[184] Gilad Lotan, Erhardt Graeff, Mike Ananny, Devin Gaffney, Ian Pearce, et al. The arab spring—the revolutions were tweeted: Information flows during the 2011 Tunisian and Egyptian revolutions. *International journal of communication*, 5:31, 2011.

[185] Emily Feng Louise Lucas. Inside china's surveillance state. https://www.ft.com/content/2182eebe-8a17-11e8-bf9e-8771d5404543. [Accessed 9-2020].

[186] Alessandro Lovari and Shannon A Bowen. Social media in disaster communication: A case study of strategies, barriers, and ethical implications. *Journal of Public Affairs*, 20(1):e1967, 2020.

[187] Justin Lynch. Women fueled Sudan's revolution, but then they were pushed aside. https://www.independent.co.uk/news/world/africa/sudan-revolution-women-uprising-democratic-transition-army-bashir-a9038786.html, 8 2019. [Accessed Aug. 2020].

[188] StopCorona. https://stopcorona.app/.

[189] Mary Madden. Privacy, security, and digital inequality: How technology experiences and resources vary by socioeconomic status, race, and ethnicity. Data & Society, September 2017. https://datasociety.net/output/privacy-security-and-digital-inequality/.

[190] Mirca Madianou. Digital inequality and second-order disasters: Social media in the Typhoon Haiyan recovery. *Social Media+ Society*, 1(2):2056305115603386, 2015.

[191] Mirca Madianou, Jonathan Corpus Ong, Liezel Longboan, and Jayeel S Cornelio. The appearance of accountability: Communication technologies and power asymmetries in

humanitarian aid and disaster recovery. *Journal of Communication*, 66(6):960–981, 2016.

[192] Raheela Mahomed and Rym Bendimerad. Venezuela shuts down internet amid protests. `https://www.aljazeera.com/news/2019/01/venezuela-shuts-internet-protests-190124124829727.html`, 1 2019. [Accessed Aug. 2020].

[193] William R. Marczak, John Scott-Railton, Morgan Marquis-Boire, and Vern Paxson. When governments hack opponents: A look at actors and technology. In *23rd USENIX Security Symposium*, 2014.

[194] Tara Matthews, Kathleen O'Leary, Anna Turner, Manya Sleeper, Jill Palzkill Woelfer, Martin Shelton, Cori Manthorne, Elizabeth F Churchill, and Sunny Consolvo. Stories from survivors: Privacy & security practices when coping with intimate partner abuse. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, pages 2189–2201, 2017.

[195] Tara Matthews, Kathleen O'Leary, Anna Turner, Manya Sleeper, Jill Palzkill Woelfer, Martin Shelton, Cori Manthorne, Elizabeth F. Churchill, and Sunny Consolvo. Stories from survivors: Privacy & security practices when coping with intimate partner abuse. In *CHI Conference on Human Factors in Computing Systems*, 2017.

[196] Allison McDonald, Catherine Barwulor, Michelle L Mazurek, Florian Schaub, and Elissa M Redmiles. "It's stressful having all these phones": Investigating sex workers' safety goals, risks, and practices online. In *30th USENIX Security Symposium (USENIX Security 21)*, 2021.

[197] Susan E McGregor, Polina Charters, Tobin Holliday, and Franziska Roesner. Investigating the computer security practices and needs of journalists. In Jaeyeon Jung Jung and Thorsten Holz, editors, *Proceedings of the 24th USENIX Security*, pages 399–414. USENIX.

[198] Susan E McGregor, Polina Charters, Tobin Holliday, and Franziska Roesner. Investigating the computer security practices and needs of journalists. In *USENIX Security Symposium*, pages 399–414, 2015.

[199] Sarah Mervosh, Jasmine C. Lee, Lazaro Gamio, and Nadja Popovich. See which states are reopening and which are still shut down. *The New York Times*. [accessed on 6-May-2020].

[200] Justin Meyers. Quickly disable fingerprints & smart lock in Android Pie for extra security. `https://android.gadgethacks.com/how-to/quickly-disable-fingerprints-smart-lock-android-pie-for-extra-security-0183475/`, 3 2018. [Accessed Aug. 2020].

[201] Volodymyr V Mihunov, Nina SN Lam, Lei Zou, Zheye Wang, and Kejin Wang. Use of twitter in disaster rescue: lessons learned from hurricane harvey. *International Journal of Digital Earth*, 13(12):1454–1466, 2020.

[202] Paul Mozur. In Hong Kong protests, faces become weapons. `https://www.nytimes.com/2019/07/26/technology/hong-kong-protests-facial-recognition-surveillance.html`. [Accessed Sep. 2020].

[203] Paul Mozur, Raymond Zhong, and Aaron Krolik. In coronavirus fight, China gives citizens a color code, with red flags. *The New York Times*, March 2020.

[204] Dhiraj Murthy and Alexander J Gross. Social media processes in disasters: Implications of emergent technology use. *Social science research*, 63:356–370, 2017.

[205] Abdelaziz Mohammed Abdelaziz Musa and Lumyaa Kamaleldeen Majzoub. The state of Sudan digital 2019. `https://sudandigital.com/portfolio/sudan-report-2019-the-state-of-sudan-digital/`, 6 2020. [Accessed Sep. 2020].

[206] Moses Namara, Daricia Wilkinson, Kelly Caine, and Bart P Knijnenburg. Emotional and practical considerations towards the adoption and abandonment of vpns

as a privacy-enhancing technology. *Proceedings on Privacy Enhancing Technologies*, 2020(1):83–102, 2020. Sciendo.

[207] United Nations High Commissioner for Refugees (UNHCR). Figures at a glance. https://www.unhcr.org/en-us/figures-at-a-glance.html, 2017. [Accessed 2-May-2022].

[208] NetBlocks Org. Study shows extent of Sudan internet disruptions amid demonstrations. https://netblocks.org/reports/study-shows-impact-of-sudan-internet-disruptions-amid-demonstrations-qr8Vj485. [Accessed Sep. 2020].

[209] Lily Hay Newman. How the Iranian government shut off the internet. https://www.wired.com/story/iran-internet-shutoff/, 1 2019. [Accessed Aug. 2020].

[210] Lily Hay Newman. Belarus has shut down the internet amid a controversial election. https://www.wired.com/story/belarus-internet-outage-election/, 10 2020. [Accessed Aug. 2020].

[211] NOAA. What is the difference between a hurricane and a typhoon? https://oceanservice.noaa.gov/facts/cyclone.html, February 2021. Accessed April 19 2022.

[212] Care19 app. https://ndresponse.gov/covid-19-resources/care19.

[213] Smittestop. https://helsenorge.no/coronavirus/smittestop.

[214] National Oceanic and Atmospheric Administration (NOAA). Tropical cyclone climatology. https://www.nhc.noaa.gov/climo/. [Accessed 25-March-2022].

[215] National Oceanic and Atmospheric Administration (NOAA). NOAA national centers for environmental information (NCEI) U.S. billion-dollar weather and climate disasters. https://www.ncdc.noaa.gov/billions/, 2022. [Accessed 7-January-2022].

[216] Onook Oh, Manish Agrawal, and H Raghav Rao. Information control and terrorism: Tracking the mumbai terrorist attack through twitter. *Information Systems Frontiers*, 13(1):33–43, 2011.

[217] Daniela Oliveira, Harold Rocha, Huizi Yang, Donovan Ellis, Sandeep Dommaraju, Melis Muradoglu, Devon Weir, Adam Soliman, Tian Lin, and Natalie Ebner. Dissecting spear phishing emails for older vs young adults: On the interplay of weapons of influence and life domains in predicting susceptibility to phishing. In *CHI Conference on Human Factors in Computing Systems*, 2017.

[218] Judith S Olson and Wendy A Kellogg. *Ways of Knowing in HCI*, volume 2. Springer, 2014.

[219] Patrick Howell O'Neill. No, coronavirus apps don't need 60% adoption to be effective. https://www.technologyreview.com/2020/06/05/1002775/covid-apps-effective-at-less-than-60-percent-download/, 6 2020. [Accessed 14-November-2020].

[220] Patrick Howell O'Neill, Tate Ryan-Mosley, and Bobbie Johnson. MIT Technology Review Covid tracing tracker. https://docs.google.com/spreadsheets/d/1ATalASO8KtZMx__zJREoOvFhOnmB-sAqJ1-CjVRSCOw/. [Accessed 14-November-2020].

[221] World Health Organization. https://covid19.who.int/table. [Accessed 14-November-2020].

[222] Michael Edmund O'Callaghan, Jim Buckley, Brian Fitzgerald, Kevin Johnson, John Laffey, Bairbre McNicholas, Bashar Nuseibeh, Derek O'Keeffe, Ian O'Keeffe, Abdul Razzaq, et al. A national survey of attitudes to COVID-19 digital contact tracing in the Republic of Ireland. *Irish Journal of Medical Science (1971-)*, pages 1–25, 2020.

[223] Leysia Palen, Sarah Vieweg, and Kenneth Mark Anderson. Supporting "everyday

analysts" in safety-and time-critical situations. *The Information Society*, 27(1):52–62, 2011.

[224] Martine Panzica. A difficult line to walk: NGO and LGBTQ+ refugee experiences with information and communications technology (ICT) in Canada. Master's thesis, Dalhousie University, 2020.

[225] Andrea Parker, Vasudhara Kantroo, Hee Rin Lee, Miguel Osornio, Mansi Sharma, and Rebecca Grinter. Health promotion as activism: building community capacity to effect social change. In Joseph A. Konstan, Ed H. Chi, and Kristina Höök, editors, *Proceedings of the 2012 ACM SIGCHI CHI*, pages 99–108. ACM.

[226] Lois Parshley. The magnitude of America's contact tracing crisis is hard to overstate. `https://www.nationalgeographic.com/science/2020/09/contact-tracing-crisis-magnitude-hot-mess-america-fixes-coronavirus-cvd/`, September 2020. [Accessed 19-November-2020].

[227] Richard J. Pasch, Robbie Berg, and Andrew B. Hagen. National hurricane center tropical cyclone report: Hurricane Henri, January 2022.

[228] Jason Patinkin. Inside the massive sit-in fueling Sudan's revolution. `https://www.vice.com/en_us/article/7xg89g/inside-the-massive-sit-in-fueling-sudans-revolution`. [Accessed Sep. 2020].

[229] Sandy Patton. How to be prepared for a natural disaster. `https://selecthealth.org/blog/2017/09/how-to-be-prepared-for-a-natural-disaster`, September 2017. [Accessed 1-April-2021].

[230] Eyal Peer, Laura Brandimarte, Sonam Samat, and Alessandro Acquisti. Beyond the turk: Alternative platforms for crowdsourcing behavioral research. *Journal of Experimental Social Psychology*, 70:153–163, 2017.

[231] Ann Peterson Bishop and Karen E Fisher. Using ICT design to learn about immigrant teens from Myanmar. In *Proceedings of the Seventh International Conference on Information and Communication Technologies and Development*, page 56. ACM, 2015.

[232] Oliver Portillo. To liberate and lament: The duality of digital culture and Chechnya's concentration camps for Russian LGBT citizens. *EXCLAMATION*, page 59, 6 2018.

[233] Emilee Rader, Rick Wash, and Brandon Brooks. Stories as informal lessons about security. In Lorrie Faith Cranor, editor, *Proceedings of the 8th SOUPS*, pages 1–17. USENIX.

[234] Radio Dabanga. Google apps available in Sudan as US eases sanctions. `https://www.dabangasudan.org/en/all-news/article/google-apps-available-in-sudan-as-us-eases-sanctions`. [Accessed Aug. 2020].

[235] Yasmeen Rashidi, Kami Vaniea, and L Jean Camp. Understanding Saudis' privacy concerns when using Whatsapp. In Tara Whalen, editor, *Proceedings of the 2016 USEC Workshop*, pages 1–8. Internet Society (ISOC).

[236] Ramesh Raskar, Isabel Schunemann, Rachel Barbar, Kristen Vilcans, Jim Gray, Praneeth Vepakomma, Suraj Kapa, Andrea Nuzzo, Rajiv Gupta, Alex Berke, Dazza Greenwood, Christian Keegan, Shriank Kanaparti, Robson Beaudry, David Stansbury, Beatriz Botero Arcila, Rishank Kanaparti, Vitor Pamplona, Francesco M Benedetti, Alina Clough, Riddhiman Das, Kaushal Jain, Khahlil Louisy, Greg Nadeau, Vitor Pamplona, Steve Penrod, Yasaman Rajaee, Abhishek Singh, Greg Storm, and John Werner. Apps gone rogue: Maintaining personal privacy in an epidemic, 2020.

[237] Ben Rawlence. *City of thorns: Nine lives in the world's largest refugee camp*. Picador, 2016.

[238] Elissa M. Redmiles. What does it mean for a COVID app to "work"? `http://www.cs.umd.edu/~eredmiles/how-good-good-enough.pdf`.

[239] Elissa M. Redmiles. User concerns & tradeoffs in technology-facilitated COVID-19 response. 2(1), 2020.

[240] Elissa M Redmiles, Yasemin Acar, Sascha Fahl, and Michelle L Mazurek. A summary of survey methodology best practices for security and privacy researchers. Technical report, 2017.

[241] Elissa M. Redmiles, Sean Kross, and Michelle L. Mazurek. How I learned to be secure: A census-representative survey of security advice sources and behavior. In *ACM Conference on Computer and Communications Security*, 2016.

[242] Elissa M. Redmiles, Sean Kross, and Michelle L. Mazurek. Where is the digital divide?: A survey of security, privacy, and socioeconomics. In *CHI Conference on Human Factors in Computing Systems*, 2017.

[243] Elissa M Redmiles, Sean Kross, and Michelle L Mazurek. How well do my results generalize? Comparing security and privacy survey results from mturk, web, and telephone samples. In *2019 IEEE Symposium on Security and Privacy (SP)*, pages 1326–1343. IEEE, 2019.

[244] Elissa M. Redmiles, Amelia R. Malone, and Michelle L. Mazurek. I think they're trying to tell me something: Advice sources and selection for digital security. In *IEEE Symposium on Security and Privacy*, 2016.

[245] Elissa M Redmiles, Noel Warford, Amritha Jayanti, Aravind Koneru, Sean Kross, Miraida Morales, Rock Stevens, and Michelle L Mazurek. A comprehensive quality evaluation of security and privacy advice on the web. In *29th USENIX Security Symposium (USENIX Security 20)*, pages 89–108, 2020.

[246] Jake Reichel, Fleming Peck, Mikako Inaba, Bisrat Moges, Brahmnoor Singh Chawla, and Marshini Chetty. 'I have too much respect for my elders': Understanding South African mobile users' perceptions of privacy and current behaviors on Facebook and

Whatsapp. In *29th USENIX Security Symposium (USENIX Security 20)*, pages 1949–1966, 2020.

[247] Christian Reuter and Marc-André Kaufhold. Fifteen years of social media in emergencies: a retrospective review and future directions for crisis informatics. *Journal of contingencies and crisis management*, 26(1):41–57, 2018.

[248] Reuters News. Residual U.S. sanctions keep Sudan's economy in chokehold. `https://www.reuters.com/article/sudan-economy/residual-u-s-sanctions-keep-sudans-economy-in-chokehold-idUSL5N1ZZ2NS`. [Accessed Sep. 2020].

[249] R. Rice and K. E. Pearce. Divide and diffuse: Comparing digital divide and diffusion of innovations perspectives on mobile phone adoption. *Mobile Media & Communication*, 3:401 – 424, 2015. SAGE.

[250] Matt Richtel. Egypt cuts off most internet and cell service. `https://www.nytimes.com/2011/01/29/technology/internet/29cutoff.html`. [Accessed Sep. 2020].

[251] Nicolás Rivero. US states are finally rolling out Covid-19 exposure notification apps. `https://qz.com/1912593/covid-19-exposure-notification-apps-are-coming-to-us-states/`. [Accessed 14-November-2020].

[252] Ronald L. Rivest, Hal Abelson, Jon Callas, Ran Canetti, Kevin Esvelt, Daniel Kahn Gillmor, Louise Ivers, Yael Tauman Kalai, Anna Lysyanskaya, Adam Norige, Bobby Pelletier, Ramesh Raskar, Adi Shamir, Emily Shen, Israel Soibelman, Michael Specter, Vanessa Teague, Ari Trachtenberg, Mayank Varia, Marc Viera, Daniel Weitzner, John Wilkinson, and Marc Zissman. `pact.mit.edu`.

[253] Fabrice Robinet. Welcome, refugees. Now pay back your travel loans. `https://www.nytimes.com/2019/03/15/nyregion/refugees-travel-loans.html`, March 2019. [Accessed 3-May-2022].

[254] Paul Roe. The 'value' of positive security. *Review of international studies*, pages 777–794, 2008.

[255] Everett M Rogers. *Diffusion of innovations.* Simon & Schuster Publishing, 2010.

[256] Joel Ross, Lilly Irani, M Silberman, Andrew Zaldivar, and Bill Tomlinson. Who are the crowdworkers?: Shifting demographics in Mechanical Turk. In *CHI'10 extended abstracts on Human factors in computing systems*, pages 2863–2872. ACM, 2010.

[257] Scott Ruoti, Jeff Andersen, Daniel Zappala, and Kent Seamons. Why johnny still, still can't encrypt: Evaluating the usability of a modern pgp client. *arXiv preprint arXiv:1510.08555*, 2015.

[258] Uptin Saiidi. Hong Kong is putting electronic wristbands on arriving passengers to enforce coronavirus quarantine. *CNBC*, March 2020. [Accessed 24-April-2020].

[259] Takeshi Sakaki, Makoto Okazaki, and Yutaka Matsuo. Earthquake shakes Twitter users: real-time event detection by social sensors. In *Proceedings of the 19th international conference on World wide web*, pages 851–860, 2010.

[260] Yukiko Sawaya, Mahmood Sharif, Nicolas Christin, Ayumu Kubota, Akihiro Nakarai, and Akira Yamada. Self-confidence trumps knowledge: A cross-cultural study of security behavior. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, pages 2202–2214, 2017.

[261] Stuart Schechter, A.J. Brush, and Serge Egelman. It's no secret: Measuring the security and reliability of authentication via 'secret' questions. In *IEEE Symposium on Security and Privacy*, 2009.

[262] Rob Schmitz. In Germany, high hopes for new COVID-19 contact tracing app that protects privacy. `https://www.npr.org/sections/coronavirus-live-updates/2020/04/02/825860406/in-germany-high-hopes-for-new-covid-19-`

contact-tracing-app-that-protects-privacy, April 2020. [Accessed 23-April-2020].

[263] Joni Schwartz. Disconnect to connect: emotional responses to loss of technology during Hurricane Sandy. In *Emotions, technology, and behaviors*, pages 107–122. Elsevier, 2016.

[264] Alaa Shahine and Glen Carey. U.A.E. Supports Saudi Arabia against Qatar-backed brotherhood. https://www.bloomberg.com/news/articles/2014-03-09/u-a-e-supports-saudi-arabia-against-qatar-backed-brotherhood. [Accessed Sep. 2020].

[265] Tanusree Sharma and Masooda Bashir. Use of apps in the COVID-19 response and the loss of privacy protection. *Nature Medicine*, pages 1–2, 2020.

[266] Michael D. Shear. Trump extends social distancing guidelines through end of April. https://www.nytimes.com/2020/03/29/us/politics/trump-coronavirus-guidelines.htmll, March 2020. [Accessed 23-April-2020].

[267] Steve Sheng, Levi Broderick, Colleen Alison Koranda, and Jeremy J Hyland. Why johnny still can't encrypt: evaluating the usability of email encryption software. In *Symposium On Usable Privacy and Security*, pages 3–4. ACM, 2006.

[268] Irina Shklovski, Moira Burke, Sara Kiesler, and Robert Kraut. Technology adoption and use in the aftermath of Hurricane Katrina in New Orleans. *American Behavioral Scientist*, 53(8):1228–1246, 2010.

[269] Hollie Silverman and Michael Guy. Crews work to restore power for tens of thousands as Henri drenches the Northeast. https://www.cnn.com/2021/08/23/weather/us-henri-monday/index.html, August 2021. [Accessed 25-March-2022].

[270] Lucy Simko, Jack Lucas Chang, Maggie Jiang, Ryan Calo, Franziska Roesner, and Tadayoshi Kohno. Covid-19 contact tracing and privacy: A longitudinal study of public opinion. *Digital Threats*, sep 2021.

[271] Lucy Simko, Ada Lerner, Samia Ibtasam, Franziska Roesner, and Tadayoshi Kohno. Computer security and privacy for refugees in the United States. In *2018 IEEE Symposium on Security and Privacy (SP)*, pages 409–423. IEEE, 2018.

[272] Selena Simmons-Duffin. COVID-19 contact tracing workforce barely 'inching up' as cases surge. `https://www.npr.org/sections/health-shots/2020/10/14/923468159/covid-19-contact-tracing-workforce-barely-inching-up-as-cases-surge`, October 2020. [Accessed 19-November-2020].

[273] Tomer Simon, Avishay Goldberg, and Bruria Adini. Socializing in emergencies—a review of the use of social media in emergency situations. *International Journal of Information Management*, 35(5):609–619, 2015.

[274] Natasha Singer. The hot new Covid tech is wearable and constantly tracks you. `https://www.nytimes.com/2020/11/15/technology/virus-wearable-tracker-privacy.html?referringSource=articleShare`, November 2020. [Accessed 19-November-2020].

[275] Natasha Singer and Choe Sang-Hun. As coronavirus surveillance escalates, personal privacy plummets. `https://www.nytimes.com/2020/03/23/technology/coronavirus-surveillance-tracking-privacy.html`, March 2020. [Accessed 24-March-2020].

[276] Robert Soden, David Lallemant, Perrine Hamel, and Karen Barns. Becoming interdisciplinary: Fostering critical engagement with disaster data. *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW1):1–27, 2021.

[277] Robert Soden and Austin Lord. Mapping silences, reconfiguring loss: Practices of damage assessment & repair in post-earthquake Nepal. *Proceedings of the ACM on Human-Computer Interaction*, 2(CSCW):1–21, 2018.

[278] Robert Soden and Embry Owen. Dilemmas in mutual aid: Lessons for crisis informatics from an emergent community response to the pandemic. *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW2):1–19, 2021.

[279] Ashkan Soltani, Ryan Calo, and Carl Bergstrom. Contact-tracing apps are not a solution to the COVID-19 crisis. April 2020.

[280] Jay Stanley and Jennifer Stisa Granick. The limits of location tracking in an epidemic. `https://www.aclu.org/aclu-white-paper-limits-location-tracking-epidemic`, April 2020.

[281] Kate Starbird, Jim Maddock, Mania Orand, Peg Achterman, and Robert M Mason. Rumors, false flags, and digital vigilantes: Misinformation on Twitter after the 2013 Boston marathon bombing. *IConference 2014 Proceedings*, 2014.

[282] Kate Starbird and Leysia Palen. "Voluntweeters" self-organizing by digital volunteers in times of crisis. In *Proceedings of the SIGCHI conference on human factors in computing systems*, pages 1071–1080, 2011.

[283] Rick Stella. The 6 best emergency kits for coping with severe weather or a natural disaster. `https://www.businessinsider.com/best-emergency-kit`. [Accessed 1-April-2021].

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

[285] Leo G Stewart, Ahmer Arif, and Kate Starbird. Examining trolls and polarization with a retweet network. In Srijan Kumar, Meng Jiang, Taeho Jung, Roger Luo, and Jure Leskovec, editors, *Proceedings of the 2018 ACM MIS2 Workshop*. ACM.

[286] Sudanese Professionals Association. About Us. `https://www.sudaneseprofessionals.org/en/about-us/`. [Accessed Sep. 2020].

[287] Nurul M Suhaimi, Yixuan Zhang, Mary Joseph, Miso Kim, Andrea G Parker, and Jacqueline Griffin. Investigating older adults' attitudes towards crisis informatics tools: Opportunities for enhancing community resilience during disasters. *arXiv preprint arXiv:2202.10927*, 2022.

[288] Mohamed Suliman. As Sudan transitions to democracy, urgent reforms must tackle disinformation. `https://advox.globalvoices.org/2019/10/04/as-sudan-transitions-to-democracy-urgent-reforms-must-tackle-disinformation/`. [Accessed Aug. 2020].

[289] Ruoxi Sun, Wei Wang, Minhui Xue, Gareth Tyson, Seyit Camtepe, and Damith Ranasinghe. Vetting security and privacy of global COVID-19 contact tracing applications. *arXiv preprint arXiv:2006.10933*, 2020.

[290] John D. Sutter. Libya faces internet blackouts amid protests. `http://www.cnn.com/2011/TECH/web/02/22/libya.internet/index.html`. [Accessed Sep. 2020].

[291] Borislav Tadic, Markus Rohde, Volker Wulf, and David Randall. ICT use by prominent activists in Republika Srpska. In Jofish Kaye, Allison Druin, Cliff Lampe, Dan Morris, and Juan Pablo Hourcade, editors, *Proceedings of the 2016 ACM SIGCHI CHI*, pages 3364–3377. ACM.

[292] Reem Talhouk, Syed Ishtiaque Ahmed, Volker Wulf, Clara Crivellaro, Vasilis Vlachokyriakos, and Patrick Olivier. Refugees and HCI SIG: The role of HCI in responding to the refugee crisis. In *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems*, pages 1073–1076. ACM, 2016.

[293] Reem Talhouk, Sandra Mesmar, Anja Thieme, Madeline Balaam, Patrick Olivier, Chaza Akik, and Hala Ghattas. Syrian refugees and digital health in Lebanon: Op-

portunities for improving antenatal health. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, pages 331–342. ACM, 2016.

[294] Marion Lara Tan, Raj Prasanna, Kristin Stock, Emma EH Doyle, Graham Leonard, and David Johnston. Usability factors influencing the continuance intention of disaster apps: A mixed-methods study. *International Journal of Disaster Risk Reduction*, 50:101874, 2020.

[295] Marion Lara Tan, Raj Prasanna, Kristin Stock, Emma Hudson-Doyle, Graham Leonard, and David Johnston. Mobile applications in crisis informatics literature: A systematic review. *International journal of disaster risk reduction*, 24:297–311, 2017.

[296] Leonie Maria Tanczer. Hacktivism and the male-only stereotype. *New Media & Society*, 18(8):1599–1615, 2016. SAGE.

[297] The Guardian Newspaper. WhatsApp design feature means some encrypted messages could be read by third party. `https://www.theguardian.com/technology/2017/jan/13/whatsapp-design-feature-encrypted-messages`. [Accessed Aug. 2020].

[298] Craig Timberg, Drew Harwell, and Safarpour Alauna. Most Americans are not willing or able to use an app tracking coronavirus infections. That's a problem for Big Tech's plan to slow the pandemic. *The Washington Post*, April 2020.

[299] Tracetogether. `https://www.tracetogether.gov.sg`.

[300] Carmela Troncoso, Mathias Payer, Jean-Pierre Hubaux, Marcel Salathé, James Larus, Edouard Bugnion, Wouter Lueks, Theresa Stadler, Apostolos Pyrgelis, Daniele Antonioli, Ludovic Barman, Sylvain Chatel, Kenneth Paterson, Srdjan Čapkun, David Basin, Jan Beutel, Dennis Jackson, Bart Preneel, Nigel Smart, Dave Singelee, Aysajan Abidin, Seda Guerses, Michael Veale, Cas Cremers, Reuben Binns, and Ciro Cattuto. Decentralized privacy-preserving proximity tracing. `https://github.com/DP-3T/documents/blob/master/DP3T\%20White\%20Paper.pdf`, April 2020.

[301] Kasey Tross. Emergency kits 101: How to be prepared for anything. https://www.safewise.com/blog/emergency-kits/, September 2020. [Accessed 1-April-2021].

[302] Zeynep Tufecki. In response to Guardian's irresponsible reporting on whatsapp: A plea for responsible and contextualized reporting on user security. http://technosociology.org/?page_id=1687. [Accessed Aug. 2020].

[303] Zeynep Tufekci. Social movements and governments in the digital age: Evaluating a complex landscape. *Journal of International Affairs*, 68:1, 2014. SIPA Columbia University.

[304] Zeynep Tufekci. *Twitter and tear gas: The power and fragility of networked protest*. Yale University Press, 2017.

[305] Uptodown App Store. Firechat. https://firechat.en.uptodown.com/android. [Accessed Sep. 2020].

[306] U.S. Central Intelligence Agency. The world factbook, Africa: Sudan. https://www.cia.gov/library/publications/resources/the-world-factbook/geos/su.html. [Accessed Sep. 2020].

[307] U.S. Dep. of State. State sponsors of terrorism. https://www.state.gov/state-sponsors-of-terrorism/. [Accessed Sep. 2020].

[308] U.S. Office of Foreign Assets Control. Sudan sanctions program. https://www.treasury.gov/resource-center/sanctions/Programs/Documents/sudan.pdf. [Accessed Aug. 2020].

[309] State of Utah releases "Healthy Together" beta app. https://coronavirus.utah.gov/state-of-utah-releases-healthy-together-beta-app/, April 2020.

[310] Raphael Varieras. How to use Zello for communication during a disaster. https://blog.zello.com/how-to-use-zello-for-communication-during-a-disaster, March 2020. [Accessed 11-April-2022].

[311] Maddy Varner. How do I prepare my phone for a protest? https://themarkup.org/ask-the-markup/2020/06/04/how-do-i-prepare-my-phone-for-a-protest, 6 2020. [Accessed Aug. 2020].

[312] Serge Vaudenay. Centralized or decentralized? The contact tracing dilemma. https://eprint.iacr.org/2020/531.pdf, May 2020.

[313] John-Paul Verkamp and Minaxi Gupta. Inferring mechanics of web censorship around the world. In Roger Dingledine and Joss Wright, editors, *Proceedings of the 2nd USENIX FOCI Workshop*. USENIX.

[314] Sarah Vieweg, Amanda L Hughes, Kate Starbird, and Leysia Palen. Microblogging during two natural hazards events: what Twitter may contribute to situational awareness. In *Proceedings of the SIGCHI conference on human factors in computing systems*, pages 1079–1088, 2010.

[315] Paul Wagenseil. Zoom security issues: What's gone wrong and what's been fixed. https://www.tomsguide.com/news/zoom-security-privacy-woes, March 2022. [Accessed 8-June-2022].

[316] Noel Warford, Tara Matthews, Kaitlyn Yang, Omer Akgul, Sunny Consolvo, Patrick Gage Kelley, Nathan Malkin, Michelle L Mazurek, Manya Sleeper, and Kurt Thomas. Sok: A framework for unifying at-risk user research. *arXiv preprint arXiv:2112.07047*, 2021.

[317] Rick Wash. Folk models of home computer security. In Lorrie Faith Cranor, editor, *Proceedings of the 6th SOUPS*, pages 1–16. USENIX.

[318] Rick Wash and Emilee Rader. Too much knowledge? Security beliefs and protective behaviors among united states internet users. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, 2015.

[319] Haohuang Wen, Qingchuan Zhao, Zhiqiang Lin, Dong Xuan, and Ness Shroff. A study of the privacy of Covid-19 contact tracing apps. In *International Conference on Security and Privacy in Communication Networks*, 2020.

[320] Alma Whitten and J Doug Tygar. Why johnny can't encrypt: A usability evaluation of pgp 5.0. In *USENIX security symposium*, volume 348, pages 169–184, 1999.

[321] Caroline Wiertz, Aneesh Banerjee, Oguz A Acar, and Adi Ghosh. Predicted adoption rates of contact tracing app configurations-insights from a choice-based conjoint study with a representative sample of the UK population. *Available at SSRN 3589199*, 2020.

[322] Wikipedia. `https://en.wikipedia.org/wiki/COVID-19_apps`.

[323] Wikipedia. Exposure notification. `https://en.wikipedia.org/wiki/Exposure_Notification`. [Accessed 14-November-2020].

[324] Simon N Williams, Christopher J Armitage, Tova Tampe, and Kimberly Dienes. Public attitudes towards COVID-19 contact tracing apps: A UK-based focus group study. *medRxiv*, 2020.

[325] Wirecutter. The best emergency preparedness supplies. `https://www.nytimes.com/wirecutter/reviews/emergency-preparedness/`, February 2021. [Accessed 1-April-2021].

[326] Ying Xu and Carleen Maitland. Communication behaviors when displaced: A case study of Za'atari Syrian refugee camp. In *Proceedings of the Eighth International Conference on Information and Communication Technologies and Development*, page 58. ACM, 2016.

[327] Eiad Yafi and Murshidah Said. Empowering refugees in Malaysia: WhatsApp as a dominant tool. 2017.

[328] Seungwon Yang and Brenton Stewart. @ Houstonpolice: an exploratory case of Twitter during Hurricane Harvey. *Online Information Review*, 2019.

[329] George Yerousis, Konstantin Aal, Thomas von Rekowski, David W Randall, Markus Rohde, and Volker Wulf. Computer-enabled project spaces: Connecting with palestinian refugees across camp boundaries. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, pages 3749–3758. ACM, 2015.

[330] Baobao Zhang, Sarah Kreps, and Nina McMurry. Americans' perceptions of privacy and surveillance in the COVID-19 pandemic. 2020.

[331] Yixuan Zhang, Nurul Suhaimi, Rana Azghandi, Mary Amulya Joseph, Miso Kim, Jacqueline Griffin, and Andrea G Parker. Understanding the use of crisis informatics technology among older adults. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pages 1–13, 2020.

[332] Lei Zou, Nina SN Lam, Shayan Shams, Heng Cai, Michelle A Meyer, Seungwon Yang, Kisung Lee, Seung-Jong Park, and Margaret A Reams. Social and geographical disparities in Twitter use during Hurricane Harvey. *International Journal of Digital Earth*, 12(11):1300–1318, 2019.

[333] Stephen Zunes. Sudan's democratic revolution: How they did it. `https://www.nonviolenceinternational.net/zunes_on_sudan`. [Accessed Sep. 2020].

Appendix A

ADDITIONAL MATERIAL FOR: DEFENSIVE TECHNOLOGY USE DURING THE 2018-2019 SUDANESE REVOLUTION

This appendix gives the interview protocol (A.1) and codebook (A.2) that we used while conducting the research, as well as a brief glossary of political actors in the Sudanese revolution (A.3).

A.1 Interview Protocol

As the interviews were semi-structured, we worded questions in different ways in each interview. While we covered the topics listed here, we also asked other questions.

Consent process

- Brief introductions of researchers, recap. research goals
- Verbal summary of the consent form:
  - Every question is voluntary
  - We'd like to record because it makes it easier on us
  - If recording, you can ask us to turn it off at any time
- Any questions before we begin?

Post consent process, pre audio recording

- Remind participants: don't share anything you don't want to share *and* we will not publish any PII

- Ask them (again) whether they consent to recording

Interview questions The following list is our short-form interview protocol, which we had in front of us during each interview. There were 7 main topics. Sub questions are *sample* questions; we did not ask all of these questions in a single interview. We typically started with 1) and ended with 7), but the order of the rest varied based on what felt comfortable during the interview.

1. **News and information sharing.**
   - How did you follow the news about the revolution?
   - What websites/apps were your main news sources?
   - Who did you get news from? Where did they get their news? Did you talk to them in person or online?
   - What kind of news did you seek?
   - Was there anything in specific where you had a hard time finding enough information about? How did you know whether to trust the information you received?
2. **Role of technology in protecting protesters.**
   - Any non-tech advice for evading arrests, tear gas, etc.?
   - Any tech advice? (may include: burner phone, burner SIM, VPN, proxy, Tor, alternate online accounts)
   - Were you given any advice that you did not follow?
   - Do you wish you'd been given any other advice? Did you feel the need to implement more measures than advised?
   - Did you ever feel like technology put you in danger?

3. **Learning / adoption / onboarding.**

   - How did you learn the advice that we just talked about? In general, from a person or by yourself?
   - For the guidelines/advice: Did you follow that advice? Was it hard? Easy? If not, why not?
   - Who gave you that advice? How did you meet them? Why did you trust them? How technically knowledgeable are they? How did you communicate with them? How frequently? Did you have to take any precautions?
   - Was the instruction one-on-one or were others there? Was it a formal setting, like a class, or an informal setting?
   - Teaching: Did you taught anyone else do [*fill in*]?

4. **Sit in.**

   - April - June, in which ways did you use technology?
   - Who was your adversary?
   - Any things you stopped doing because you felt safe?

5. **Internet blackout.**

   - During the internet blackout in June 2019, did you continue to use technology for activism? For the things that stopped working, what did you do instead?
   - Because of the very limited internet access, did that force you as activists to share accounts, devices, etc.?
   - As a whole, how do you think the activism community changed their use of technology during the blackout?

6. **Threat model.**

- What are/were the dangers you are/were facing as an activist? Who is an adversary to you?
- If they mention the government as an adversary: what arm(s) of the government might be harmful? For each: what are their capabilities? What do you use to defend against them? Is that enough to protect you?

7. **Final / meta questions.**

- Is there anything else you want to tell us?
- Is there anything we should have asked but we didn't?
- Do you have any questions for us?
- Can you refer us to more activists?

A.2 Codebook

Next we present our codebook. We show each high level code and its subcodes. Subsubcodes are not included because they were used only for giving counts of specific actions or threat models (e.g., the subsubcode 'Electronic surveillance', which is not shown, appeared under 'Threat model and threats—Sudanese government capabilities'; we used it to report on how many participants mentioned electronic surveillance as a capability of the Sudanese government).

High-level Code	**Subcodes**	
Threat model and threats: *Refers to the activists' perceptions of who their adversaries are and what their capabilities are*	Risk assessment Changing adversaries Adversary Sudanese gov. capabilities Trigger for change in threat model	Outsourced capabilities Trusted party Asset Foreign gov. capabilities
Adoption of technology and behaviors: *Refers to activists' behaviors towards adoption and the challenges they faced*	Learning process Choice not to adopt Discontinuing use	Trigger for adoption Challenges / barriers Teaching
Mis-/disinformation security: *Refers to activists' needs and practices toward information verification*	Building trust Making information verifiable	Sources of trust Verification of information
Plausible deniability: *Refers to activists' needs and practices that provide plausible deniability upon* arrest	Built-in security mechanism Go analog Deny self access to info / regular device	Ad hoc strategy Expect others to do something Deny others access to info
Security against surveillance: *Refers to participants' needs and practices to defend against electronic surveillance*	Built-in security mechanism Go analog Deny self access to info or regular device	Ad hoc strategy Expect others to do something Deny others access to info
Physical security: *Refers to practices to maintain physical security*	*no subcodes*	

Table A.1: This table captures our codebook (part I of II).

High-level Code	**Subcodes**
Offensive security practices: *Refers to offensive practices by activists (as opposed to defensive)*	*no subcodes*
Censorship and blackout: *Refers to activists' security needs and practices during the social media blockade and internet blackout*	Blackout Social media blockade Other
News consumption operational needs & goals: *Refers to activists' news consumption*	Platform News source Type of news
Communications operational needs & goals: *Refers to participants' practices with regards to communications and news dissemination*	*subcodes = specific platforms*
Comparisons: *Refers to comparisons between previous protests/revolutions ordifferent technologies being used*	Previous protests / revolutions Preferred platform X to Y
Participant's overall experience: *Refers to anything not covered above about the participant's role in the revolution*	Was in Sudan during the revolution Not in Sudan during the revolution Role during revolution Role of diaspora

Table A.2: This table captures our codebook (part II of II).

A.3 Summary of State and Non-state Actors

Finally, we present readers with a brief glossary of actors mentioned in the main content of the paper. This is intended to support the reader throughout the paper but is in no way a complete representation of the actors in the Sudanese revolution. We invite interested readers to begin with [84, 133, 333] for more information about the forces throughout the revolution.

Sudanese Professional Association (SPA)	**Revolutionary force (ally)**: The SPA is an umbrella organization for a number of professional associations—e.g. Teachers' Committee, Central Committee of Sudanese Doctors, etc [286]—that helped publicly organize protests and push forward the revolution. The SPA was a trusted source of news throughout the revolution.
Neighborhood resistance committees	**Revolutionary force (ally)**: Neighborhood committees were decentralized local committees formed during or sometimes even before the revolution [12]. They communicated with the SPA and each other.
Transitional civilian government	**Revolutionary force (ally):** The SPA and a number of opposition political parties coalesced to form a body known as the Freedom of Forces and Change. This body was the political representation of the activism community and further helped negotiate an agreement with the Transitional Military Council to form a transitional civilian government that continues to lead the country in a democratic transition that began in July of 2019.
National Intelligence and Security Service (NISS)	**Government (adversary)**: The NISS is an intelligence unit that served as a "secret police" under Elbashir's regime. The NISS was granted extensive authority by the government and was responsible of a lot of human rights abuses throughout Elbashir's rule [21]. According to our participants, the NISS was heavily involved in repressing protesters.

Table A.3: This glossary summarizes the roles of the main actors (entities) mentioned in the chapter (part I of II). Bold text indicates the way these actors were perceived by our participants.

Rapid Support Forces (RSF)	**Government (adversary)**: The RSF are armed forces originally operating under Elbashir's government with a history of violence and human rights violations both prior to and during the revolution [15]. The RSF coalesced with the state military to form the Transitional Military Council in April 2019.
Sudanese Military	**Government (adversary)** (during sit in): The official military of the Sudanese state. In the beginning, many did not consider them an adversary; however, they started to turn adversarial during the sit in, and following the crackdown on protesters on the 3rd of June Khartoum massacre [22].
Police	**Government (adversary):** Regional / city police that were arresting protesters. However, sometimes participants used the word "police" to describe units from the NISS who were arresting protesters as well.
Transitional Military Council (TMC)	**Government (adversary)** (during sit in): The TMC was formed following the fall of Elbashir's regime to lead the country and occupy the power vacuum. The council consisted of the state military and the Rapid Support Forces (RSF). During this period the NISS was stripped of its authority and remained idle.
Saudi Arabia	**Foreign power (adversary)**: The government of Saudi Arabia supported Elbashir's regime. In the early days of the revolution, Saudi Arabia reinstated support for the Sudanese government and for stability in the region. After the fall of the regime in April, Saudi Arabia became an ally to the Transitional Military Council (TMC), pledging millions of dollars in support of the council and pushing for military rule.
United Arab Emirates (UAE)	**Foreign power (adversary)**: The UAE was among a number of foreign powers supporting the Sudanese government as the protests erupted by helping the Sudanese economy. They also financially supported the TMC.
Qatar	**Foreign power (adversary)**: In January of 2019, the Emir of Qatar emphasized their support for Elbashir's rule.
Egypt	**Foreign power (adversary)**: Egypt was a strong regional ally of Elbashir's government throughout the revolution.
Muslim Brotherhood	**Domestic and foreign movement:** The Muslim Brotherhood is a multi-national political group backed by Turkey and Qatar, and considered as terrorists by others, including the UAE, Saudi Arabia, and Egypt [31, 264].

Table A.4: This glossary summarizes the roles of the main actors (entities) mentioned in the chapter (part II of II). Bold text indicates the way these actors were perceived by our participants.

Appendix B

SURVEY PROTOCOL FOR: COVID-19 CONTACT TRACING AND PRIVACY: A LONGITUDINAL STUDY OF PUBLIC OPINION

B.1 Survey Protocol

The latest version of the survey protocol is below, with footnotes marking questions that were not present in some earlier versions. We give section headings and descriptors for the reader's reference here; participants did not see headers. Unless otherwise specified, all questions were answered on a five-point Likert scale.

The logo of our institution (with the institution name prominent) appear as a header to each survey page. Our lab and department name did not.

Throughout the course of this research, we became aware of some inconsistencies or ambiguities in the questions. We chose not to revise the protocol to address these issues, in order to preserve the ability to do longitudinal comparisons. We present the protocol here as it was presented to participants so that the reader can understand what participants experienced.

B.1.1 Consent and Screening

This is a survey about **location tracking and Coronavirus (COVID-19)** by researchers at the University of Washington, in Seattle. University of Washington's Human Subjects Division reviewed our study, and determined that it was exempt from federal human subjects regulation. We do not expect that this survey will put you at any risk for harm, and you don't have to answer any question that makes you uncomfortable. In order to participate, you must be at least 18 years old, regularly use a smartphone, and able to complete the survey in English. We expect this survey will take about 15-20 minutes to complete.

If you have any questions about this survey, you may email us at ¡study-specific-email¿.

Thanks for taking our survey! To start, please answer the two questions below...

Are you at least 18 years old? [yes, no]

Do you use a smartphone regularly? [yes, no]

B.1.2 Demographics I

This survey involves questions about **COVID-19**, the disease caused by SARS-CoV-2 (commonly known as **coronavirus**).

Q6: How concerned are you about COVID-19?

Q7: Do you believe that social distancing is an important tool for slowing the spread of COVID-19? [yes, no, not sure]

Q8: Averaged over the past week, approximately how many hours much time per day did you spend out of your home, within 6 feet (2 meters) of other people? (e.g., getting groceries, working at an essential job like in a hospital, in a grocery store, etc). ['I did not leave my home', 0-1 hours per day, 2-3 hours per day, ... , 7-8 hours per day, 8+ hours per day]

Q144: Do you believe that wearing a mask is an important tool for slowing COVID-19? [yes, no, not sure]

Q145: Over the past week, how often did you wear a mask when you were out of your home? [All of the time, most of the time, some of the time, rarely, never]

Q9: In which country do you currently reside? [drop-down country list]

Q10: For respondents in the USA: in which state do you currently reside? [drop-down US state list]

B.1.3 Cell phone manufacturer and provider location data

Cell phone manufacturers and cellular providers have access to your physical-world location.

Q12: How comfortable are you with your cell phone manufacturer or your cellular carrier using your location data for the purposes of studying or mitigating the spread of COVID-19?

Q13: How comfortable are you with your cell phone manufacturer or your cellular carrier sharing your location data for the past two weeks **with your government** for the purposes of studying or mitigating the spread of COVID-19? (**Regardless of whether you test positive for COVID-19.**)

Q14: **If you tested positive for COVID-19**, how comfortable would you be with your cell phone manufacturer or your cellular carrier sharing your location data for the past two weeks **with your government** for the purposes of studying or mitigating the spread of COVID-19?

Q15: **If you tested positive for COVID-19**, how comfortable would you be with your cell phone manufacturer or your cellular carrier sharing your location data for the past two weeks **publicly**?

Q16: Optionally, do you have any other thoughts about your cell phone manufacturer or your cellular carrier sharing your location data for the purposes of studying or mitigating the spread of COVID-19? [free response]

B.1.4 Existing app location data

Some phone applications have access to your physical-world location, either when the application is in use or all the time. ***Suppose the makers of an existing app on your phone started using your GPS location data to study or mitigate the spread of COVID-19.*** *For example, this could include disclosing past locations of known positive COVID-19 cases to the public or to the government, or alerting people who have crossed paths with the positive case.*

Q18: Below we've listed 15 commonly-used apps. For the apps that you use regularly: how comfortable are you with the following apps using your location data for the purposes of studying or mitigating the spread of COVID-19? ["I don't use this app" + 5-point Likert scale for each of the following apps]

- Google Maps
- Apple Maps
- Waze
- Facebook
- Instagram
- TikTok
- WhatsApp
- Facebook Messenger
- Zoom
- Uber
- Lyft
- Airbnb
- Calorie Counter (MyFitnessPal)
- FitBit
- AllTrails

Suppose that one of the apps that you regularly use – not necessarily one of the ones above – started using your location data to study or mitigate the spread of COVID-19.

Q20: How comfortable are you with this app using your location data for the purposes of studying or mitigating the spread of COVID-19?

Q22: **If you tested positive for COVID-19**, how comfortable would you be with this app sharing your location data for the past two weeks **publicly**?

Q23: Consider all the apps you regularly use on your phone (not just the apps listed earlier). Which app would you **most** trust to use your location data for the purposes of studying and mitigating COVID-19? Why? [free response]

Q24: Which app that you currently use would you **least** trust to use your location data for the purposes of studying and mitigating COVID-19? Why? [free response]

B.1.5 Current use of COVID-19 app

Q25: Have you used any apps that help track the spread of COVID-19? (i.e. Singapore's "TraceTogether") [yes, no]

`If yes, participants branch to 'already have app.'`

`If no, participants continue.`

B.1.6 New app, perfect privacy

*Imagine there is a **new** app that would track your location at all times for the purposes of mitigating the spread of COVID-19.*

Suppose that this app protects your data perfectly.

Q50: How likely would you be to install and use this app?

Q51: Would this app change your current behavior?

Q52: Optionally, please use this space tell us any initial thoughts you have about such an app. [free response]

B.1.7 New app, app makers know location

Imagine there is a new app that would track your location at all times for the purposes of studying or mitigating the spread of COVID-19.

Suppose now that the makers of the application would know your location at all times, but would not share your location with any other entity.

Q55: How likely would you be to install and use this app?

Q56: Now, suppose that the app is made by one of the following companies, all of which already have created popular apps. Please rate how comfortable you would be if each company were responsible for this new app. [“I don’t know enough about this company to make a decision” + 5-pt Likert scale for each of the following]

- Google (Google Maps, Waze, etc)
- Apple (Apple Maps)
- Facebook (Facebook, Facebook Messenger, Instagram, WhatsApp)
- Microsoft (Skype, OneDrive, etc)[1]
- ByteDance (TikTok)
- Zoom Video Communication
- Uber
- Lyft
- AirBnb
- MyFitnessPal
- AllTrails
- FitBit

[1] Added April 17 (week 3).

Q57: Suppose that the app is made by one of the following general entities. Please rate how comfortable you would be if one of the following were responsible for this new app, which would use the location data they collect from your smartphone to track the spread of COVID-19. [5-pt Likert scale for each of the following]

- A university research group
- An activist group
- An industry startup
- Your government
- The United Nations

Q58: Optionally, please use the space below to elaborate on your thoughts about one or more companies using your location data for the purposes of tracking COVID-19. [free response]

B.1.8 New app, app makers share data with government

Again, imagine there is a new app that would track your location at all times for the purposes of studying or mitigating the spread of COVID-19.

Suppose now that the makers of the application would know your location at all times, and would also share that data with your government if you were diagnosed with COVID-19.

Q61: How likely would you be to install and use this app?

Q62: If the government's use of the data were **supervised by a judge**, how likely would you be to install and use this app?[2]

Now suppose that the makers of the application would share your location data with your government ***only if you tested positive for COVID-19.***

[2] This question, and the rest of this section, was added on April 17 (week 3) as a previous version was ambiguous.

Q63: How likely would you be to install and use this app?

Q112: If the government's use of the data were **supervised by a judge**, how likely would you be to install and use this app?

Q64: Optionally, do you have any other thoughts about a company that is doing COVID-19 tracking sharing your location with your government? [free response]

Q115: Optionally, do you have any other thoughts about judicial oversight of the government's usage of location data? [free response]

B.1.9 Other location data sources: Credit card history and surveillance camera footage

There[3] *are other ways to track someone's location. One is the use of video cameras in public places. Another is the use of credit card purchasing histories.*

Q115: How comfortable would you be with your **credit card company** deriving your location history for the past two weeks for the purposes of studying and mitigating the spread of COVID-19?

Q116: How comfortable would you be with your **credit card company** deriving your location history for the past two weeks **and sharing it with your government** for the purposes of studying and mitigating the spread of COVID-19?

Q117: Optionally, do you have any other thoughts about your location history being derived from your **credit card** purchase history?

B.1.10 Other data location sources II: wearable electronics and public area sensors

Suppose[4] there were an electronic bracelet that would track your location for the purposes of studying or mitigating the spread of COVID-19.

Q146: How likely would you be to use this bracelet?

[3] Added April 17 (week 3)

[4] Added July 17 (week 16)

Q147: Optionally, do you have any other thoughts about wearable electronics being used for the purposes of studying or mitigating the spread of COVID-19?

Suppose your region added sensors (such as cameras, phone tagging stations, etc) in public areas (such as subway stations, bus stops, storefronts, public parks, etc).

Q148: How comfortable would you be with the use of public-area sensors to study or mitigate the spread of COVID-19?

Q149: Optionally, do you have any other thoughts about such sensors being used for the purposes of studying or mitigating COVID-19?

B.1.11 Proximity tracing

One alternative[5] *to location tracking for the purposes of studying or mitigating COVID-19 is* ***proximity tracing****, in which your phone would automatically exchange information with every phone within 6 feet (2 meters) of your phone,* ***keeping track of your close physical encounters, but not tracking your actual location****. This data could then be used to reconstruct your close encounters if you contracted COVID-19, or could alert you if someone you had been in close physical proximity to tested positive for COVID-19.*

Q121: Imagine that your **cell phone manufacturer or phone operating system** would conduct proximity tracing for the purposes of studying or mitigating COVID-19 (and, vice versa, other phones will record that they have been in the proximity of your phone). How comfortable would you be with this?

Q122: Suppose that your **cell phone manufacturer or phone operating system** would share this proximity data **with your government** if you tested positive for COVID-19. How comfortable would you be with this?

Q123: Optionally, do you have any other thoughts about your cell phone manufacturer or phone operating system tracking other phones nearby? [free response]

Imagine instead there is a new ***app*** *that would conduct proximity tracing for the purposes*

[5] Added April 17 (week 3)

of studying or mitigating COVID-19: that is, it would not track your location, but would instead keep track of other phones that you are nearby (and, vice versa, other phones with this app will record that they have been in the proximity of your phone).

Q124: How likely would you be to download this app?

Q125: Now, suppose that the proximity tracing app is made by one of the following companies. Please rate how comfortable you would be if each company were responsible for this new app. [“I don’t know enough about this company to make a decision” + 5-pt Likert scale for each of the following]

- Google (Google Maps, Waze, etc)
- Apple (Apple Maps)
- Facebook (Facebook, Facebook Messenger, Instagram, WhatsApp)
- Microsoft (Skype, etc)
- ByteDance (TikTok)
- Zoom Video Communication
- Uber
- Lyft
- AirBnb
- MyFitnessPal
- AllTrails
- FitBit

Q126: Now, suppose that the proximity tracing app is made by one of the following general entities. Please rate how comfortable you would be if each entity were responsible for this new app.

- A university research group
- An activist group
- An industry startup
- Your government
- The United nations

Q127: Optionally, do you have any other thoughts about an app that tracks other phones nearby?

Q128: Optionally, do you have any other thoughts about proximity tracking versus location tracking for the purposes of studying or mitigating COVID-19?

B.1.12 Government use of data

If the government acquired your location data or proximity data[6] *(i.e. from an app on your phone, from your cell phone carrier, etc)* ***for the purposes for studying and mitigating COVID-19****....*

Q66: How likely do you think it is that your government would **delete** the data after the pandemic ends?

Q67: How likely do you think it is that your government would **only** use the data for the purposes of tracking COVID-19?

Q68: How concerned would you be about your government's use of your location data harming **your personal safety** or the safety of those in your community?

[6] 'or proximity data' added April 17

Q69: Suppose your location was shared with only a specific sector of the government. For each of the following sectors of government, please rate how comfortable you would be with them having access to your location data.

- Federal Disease Tracking Agency (US: CDC)
- Your state or City Health Department
- Tax Agency (US: IRS)
- Local law enforcement (state, country, city, etc)
- Immigration authorities (US: CBP or ICE)

Q70: Optionally, please use the space below to elaborate on your thoughts about the government having access to your location data for the purposes of COVID-19 tracking. [free response]

B.1.13 App features

In some countries, such as South Korea, China, and Singapore, there do exist apps to monitor the spread of COVID-19 through location tracking. These apps can have multiple purposes, including:

- Alerting the user if they have come into contact with someone who later tests positive with COVID-19;

- Helping the community or law enforcement enforce isolation and quarantine edicts;

- Tracing viral strains through the community.

Q72: If a new app were deployed in your country to mitigate the spread of COVID-19, which of the following features would you want it to have? (5-point Likert-scale for each of the following:)

- Notify you if you came close to someone who later tested positive for COVID-19

- Notify anyone you came close to in the past two weeks if you tested positive for COVID-19
- Make your location history for the past two weeks publicly available if you tested positive for COVID-19
- Make public a database of the location histories of anyone who tested positive for COVID-19
- Notify you if your neighbors were not isolating themselves as recommended or mandated
- Let you notify the authorities if you saw people you suspected or knew to be breaking the isolation recommended or mandated
- Automatically notify the authorities if people were not isolating as mandated
- Used by scientists to study tends, not individuals
- Geofence to enforce mandatory or voluntary quarantine
- General assessment of social distancing in an area to display areas of high congregation

Q73: Optionally, do you have any other thoughts about what you would want such an app to do? [free response]

Q74: Optionally, do you have any other thoughts about what you would want such an app to NOT do? [free response]

Q75: Is such an app available in your country? [Yes / No / I'm not sure]

`If yes, participants branch to 'App available'`

B.1.14 Prior privacy preferences

We're now going to ask you about your thoughts about location sharing with your government BEFORE COVID-19.

Q80: In Oct 2019 (before the first known cases of COVID-19), how comfortable would you have been with your location data being shared with the government in general?

Q81: In Oct 2019 (before the first known cases of COVID-19), how comfortable were you with your location data being shared with the following sectors of government? [5-Point Likert scale for each of the following:]

- Federal Disease Tracking Agency (US: CDC)
- Your state or City Health Department
- Tax Agency (US: IRS)
- Local law enforcement (state, country, city, etc)
- Immigration authorities (US: CBP or ICE)

Q82: Optionally, please use the space below to elaborate on your thoughts about one or more companies sharing your location data with some part of the government (before COVID-19). [free response]

B.1.15 Demographics II

Almost done!

Q39: What is your age? (you may answer approximately if you do not know, or wish not to say exactly) [free response]

Q40: What is your gender identity? [free response]

Q141: Please select any races or ethnicities that you feel accurately reflect who you are. Please select as many as apply to you. We also realize that because race and ethnicity cannot be put into categories, you may prefer to self-describe your race and ethnicity in the following question. You may also select from the options below and submit a free-response. The following races and ethnicities are presented in alphabetical order. [American Indian or Alaskan Native, Asian, Black or African American, Hispanic, Native Hawaiian or Other Pacific Islander, White][7]

Q142: If you prefer to self-describe your race and ethnicity instead of or in addition to using the checkboxes above, please do so here. [free response][8]

Q41: What political party do your views typically align with? [free response]

Q42: What are your top three news sources? (i.e. Twitter, Facebook, Fox News, CNN, NPR, New York Times, etc) [free response]

Q132: Have you ever had COVID-19? [Yes, definitely; Yes, I think so; I am unsure; No, I don't think so; No, definitely not][9]

Q133: Have you ever been medically tested for COVID-19? [Yes, I have had a test; No, I have not been tested][10]

Q43: Regarding COVID-19, are you in high risk group or live with someone with high risk? [yes / no]

Q44: Are you generally interested in or concerned about privacy and technology? [yes / no]

Q45: Do you know how to change location permissions for apps on your phone? [yes / no]

Q129: What is your phone manufacturer? (e.g. Apple, Samsung, Huawei, Nokia, OnePlus, XiaoMi, OPPO, etc) [free response][11]

[7] Added week 12

[8] Added week 12

[9] Added week 5

[10] Added week 5

[11] Added week 5

B.1.16 Branch: app is available

Q76: Have you downloaded the app in your country to mitigate or study the spread of COVID-19? [yes, no]

Q77: If you have not downloaded the app: why not? what changes, or assurances by the manufacturer or government (if any) would you want to see to the app before downloading? [free response]

Q78: What are your thoughts about the privacy properties of this app? [free response]

B.1.17 Branch: Already have app

You indicated that there is an app (or apps) available in your country to track, study, or mitigate COVID-19. This section will ask about that app.

Q27: What is the name of the app, or apps?

Q28: Why did you install and use it?

Q29: Do you know anyone who did not download the app? [yes, no]

Q30: If so, why did they not install it?

Q31: What concerns, if any, do you have about the app?

Q32: If you had or have concerns, what outweighed the concerns and lead you to the decision to download the app?

Q33: What concerns, if any, do you have about your government having access to your location data?

Q34: What concerns, if any, do you have about the app makers having access to your location data?

Q35: Do you expect the app makers to stop storing your location data after the pandemic is over?

Q36: Do you plan to delete the app after the pandemic?

Q37: Anything else you'd like to say about the app and/or your concerns?

Appendix C

ADDITIONAL MATERIAL FOR: THE USE AND DISUSE OF TECHNOLOGY DURING HURRICANES

C.1 Hurricane Survey Modules

There were 3 different surveys in this project, comprised of similar/the same questions. I present the modules here, then show how they fit together.

Survey flow information is denoted by `text like this`.

C.1.1 General preparation module

Q1 What natural disasters occur in your area?

- Floods
- Wildfires
- Cyclones, hurricanes, and/or tropical storms
- Blizzards and/or ice storms
- Droughts
- Extreme cold
- Extreme heat
- Tornados

Q2 In general, how do you and your household prepare for natural disasters / extreme weather?

- We stock extra food and/or water
- We stock supplies to create a temporary shelter (e.g., tent, plastic sheeting, duct tape)

- We stock external sources of power or light (e.g., batteries, generator, candles)
- We stock medical or sanitary supplies (e.g., first aid kit, medications, contact solution)
- We stock extra currency (e.g., cash, travelers checks, etc)
- We have weapons prepared (e.g., pepper spray, firearms)
- We physically prepare our home or community
- We plan with others in our community
- We make specific preparations for our pets (e.g., extra food, backup power for aquariums, etc)

Q3 What technology or information-related preparations do you and your household make for natural disasters / extreme weather?

- We put paper copies of important or sentimental documents in a certain safe and/or accessible place (e.g., identification, insurance deeds, etc)
- We maintain or update digital copies of important or sentimental documents (e.g., in the cloud, on a portable USB drive in a safe place, etc)
- We download certain apps or software (e.g., FEMA app, local weather app, Google offline maps)
- We keep backups of authentication methods (e.g., written copies of important passwords, written copies of multi-factor authentication codes, alternative hardware authentication devices)
- We have external smartphone batteries
- We keep alternate two-way communication methods (e.g., standalone mobile hotspot, pocket WiFi, satellite phone, two-way radio)

Q4 If there is anything else that you do (or plan to do) to prepare for a natural disaster, please write a sentence or two here about it:

Q5 If there are any preparations that you would *like* to do, but you cannot for some reason, please write a few sentences here: (a) what would you like to do to prepare, and (b) why can you not do it?

`Q6 displayed if more than 1 box from Q2 is checked`

Q6 In general, how did you learn about (or decide to do) these preparations? Check all that apply.

- friend or family member
- neighbor or community member
- online search about disaster preparation or something similar other online search
- news story
- online ad
- offline ad (e.g., billboard, newspaper ad, etc)
- public service announcement
- informational website: *[free response box]*
- applied from other aspects of my life
- I previously experienced a hardship in which I needed or wanted this
- Other *[free response box]*

`Q7 and Q8 are displayed if the corresponding box from Q3 is checked`

Q7 You indicated that you keep paper copies of documents. Please tell us briefly about (a) how you store the documents safely, and (b) what sort of documents you have stored.

Q8 How did you learn (or decide) to keep paper copies of important documents as part of your disaster preparation? Check all that apply.

- friend or family member
- neighbor or community member
- online search about disaster preparation or something similar other online search
- news story
- online ad

- offline ad (e.g., billboard, newspaper ad, etc)
- public service announcement
- informational website: *[free response box]*
- applied from other aspects of my life
- I previously experienced a hardship in which I needed or wanted this
- Other *[free response box]*

`Q9 and Q10 are displayed if the corresponding box from Q3 is checked`

You indicated that you keep digital copies of documents.

Q9 Please tell us briefly about (a) what kind of storage you are using (e.g., the cloud, USB), and (b) what sort of documents you have stored digitally.

Q10 How did you learn (or decide) to keep digital copies of important documents as part of your disaster preparation? Check all that apply.

- friend or family member
- neighbor or community member
- online search about disaster preparation or something similar other online search
- news story
- online ad
- offline ad (e.g., billboard, newspaper ad, etc)
- public service announcement
- informational website: *[free response box]*
- applied from other aspects of my life
- I previously experienced a hardship in which I needed or wanted this
- Other *[free response box]*

`Q11 and Q12 are displayed if the corresponding box from Q3 is checked`

You indicated that you have downloaded or plan to download certain apps or software as part of your disaster preparation.

Q11 What apps or software do you (or did you) download? Please be specific and write as many as you can remember.

Q12 How did you learn about (or decide to download) these apps? Please check all that apply.

- friend or family member
- neighbor or community member
- online search about disaster preparation or something similar other online search
- news story
- online ad
- offline ad (e.g., billboard, newspaper ad, etc)
- public service announcement
- informational website: *[free response box]*
- applied from other aspects of my life
- I previously experienced a hardship in which I needed or wanted this
- Other *[free response box]*

`Q13 and Q14 are displayed if the corresponding box from Q3 is checked`

You indicated that you keep backups of authentication methods.

Q13 Please tell us briefly what those backups are. Note: this question is not asking you for your passwords; we are asking if, for example, you keep a copy of your passwords in or near your emergency kit, or if you use a cloud-based password manager. Do not tell us your passwords.

Q14 How did you learn (or decide) to keep backups of authentication methods? Please check all that apply.

- friend or family member
- neighbor or community member
- online search about disaster preparation or something similar other online search

- news story
- online ad
- offline ad (e.g., billboard, newspaper ad, etc)
- public service announcement
- informational website: *[free response box]*
- applied from other aspects of my life
- I previously experienced a hardship in which I needed or wanted this
- Other *[free response box]*

`Q15 and Q16 displayed if the corresponding box from Q3 is checked`

You indicated that you keep external smartphone batteries.

Q15 Please write a sentence or two about how these fit into your disaster plan. For example: how many do you have, when do you charge them, do you use them for other purposes, etc.

Q16 How did you learn (or decide) to acquire these technologies? Please check all that apply.

- friend or family member
- neighbor or community member
- online search about disaster preparation or something similar other online search
- news story
- online ad
- offline ad (e.g., billboard, newspaper ad, etc)
- public service announcement
- informational website: *[free response box]*
- applied from other aspects of my life
- I previously experienced a hardship in which I needed or wanted this
- Other *[free response box]*

`Q17 and Q18 are displayed if the corresponding box from Q3 is checked`

You indicated that you keep alternate two-way communication technologies (e.g., standalone WiFi hotspot, pocket WiFi, satellite phone, two-way radio, etc).

Q17 Please tell us specifically what those technologies are.

Q18 How did you learn (or decide) to acquire these technologies? Please check all that apply.

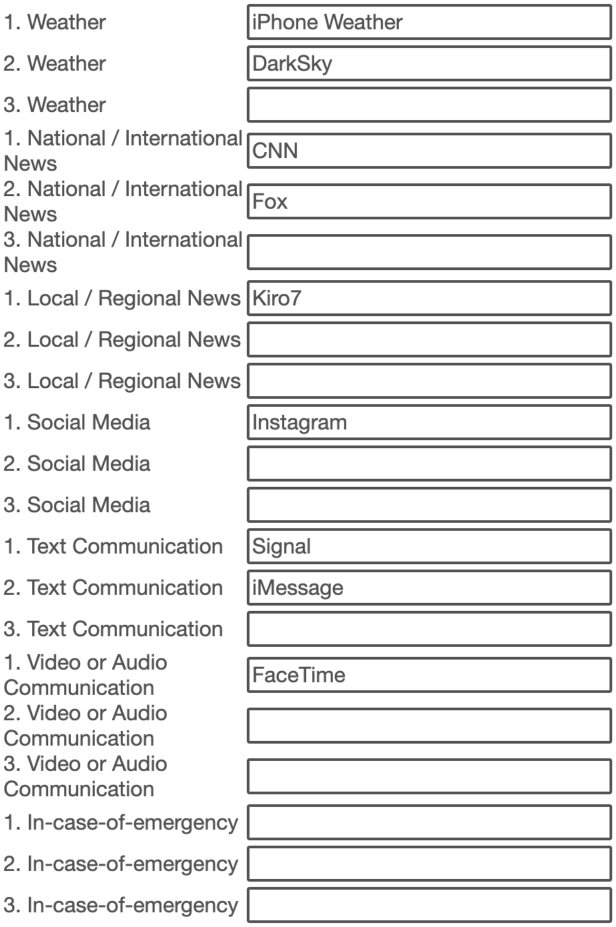
- friend or family member
- neighbor or community member
- online search about disaster preparation or something similar other online search
- news story
- online ad
- offline ad (e.g., billboard, newspaper ad, etc)
- public service announcement
- informational website: *[free response box]*
- applied from other aspects of my life
- I previously experienced a hardship in which I needed or wanted this
- Other *[free response box]*

Q19 If you had any issues with the questions in this section, please let us know here!

C.1.2 Apps used during everyday life and/or a specific disaster

Q1 Please tell us the names of 3 apps or websites you use in each of the following categories. Please put down apps that you use frequently either during a crisis, or during non-crisis times, or both. *Note: It's fine to leave some blank if you don't have 3 apps in a category; if one app fits in multiple categories you only need to input it once.* ***You must input at least one app.***

`Participants wrote any number of apps in the 21 spaces shown in Figure C.1. There were three spaces for apps in each of the seven following categories:`



1. Weather	iPhone Weather
2. Weather	DarkSky
3. Weather	
1. National / International News	CNN
2. National / International News	Fox
3. National / International News	
1. Local / Regional News	Kiro7
2. Local / Regional News	
3. Local / Regional News	
1. Social Media	Instagram
2. Social Media	
3. Social Media	
1. Text Communication	Signal
2. Text Communication	iMessage
3. Text Communication	
1. Video or Audio Communication	FaceTime
2. Video or Audio Communication	
3. Video or Audio Communication	
1. In-case-of-emergency	
2. In-case-of-emergency	
3. In-case-of-emergency	

Figure C.1: Screenshot of the Qualtrics interface where participants entered apps they have used, with example data (data not shown to participants)

weather, national / international news, local / regional news, social media, text communication, video or audio communication, in-case-of-emergency

One survey employed a filter question here to ascertain whether participants had experienced a disaster in the past 10 years.

We then showed participants the apps they had entered next to three categories about how they had used the apps and asked participants to sort the apps into the appropriate categories, as shown in Figure C.2

Q2 Please drag the app names into the appropriate categories (order does not matter).

Categories:

[Scenario A] I have used this app during a disaster, but not during everyday life
[Scenario B] I have used this app during everyday life, but not during a disaster
[Scenario C] I have used this app during both a disaster and everyday life

We then asked free-response questions about the categories of apps:

SCENARIO A:

Q3 What did you use these apps for?

Q4 Did you encounter any issues or have any concerns with these apps?

SCENARIO B:

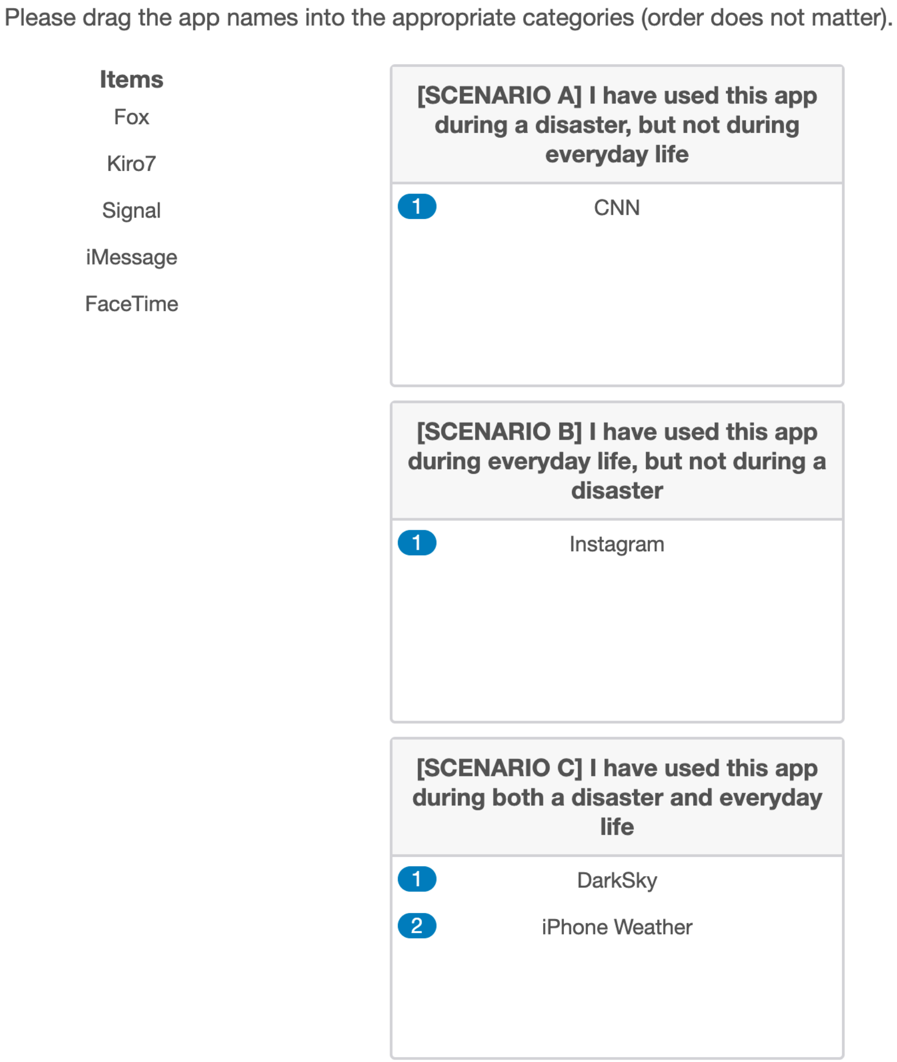
Q5 Please briefly explain why you could NOT use these apps or website during the disaster, or why you choose not to.

SCENARIO C:

Q6 How did you use these apps during the disaster?

Q7 Did you encounter any issues or concerns with these apps or websites during the disaster?

Q8 If you had any issues with the questions in this section, please let us know here



Please drag the app names into the appropriate categories (order does not matter).

Items

Fox

Kiro7

Signal

iMessage

FaceTime

[SCENARIO A] I have used this app during a disaster, but not during everyday life

1 CNN

[SCENARIO B] I have used this app during everyday life, but not during a disaster

1 Instagram

[SCENARIO C] I have used this app during both a disaster and everyday life

1 DarkSky

2 iPhone Weather

Figure C.2: Screenshot of the Qualtrics interface where participants sorted the apps they had entered previously, with example data (data not shown to participants)

C.1.3 Reflections on use of technology during the disaster

Our survey evolved after our baseline run because we thought, based on pilot interviews and surveys, that participants might be able to answer more specific free response questions more immediately after or during a disaster. Both versions of this question broadly cover self-reported changes in technology use during a storm. The questions from the survey deployed at the start of hurricane season then ask specifically security and privacy issues, while the questions from the survey deployed during and immediately after a hurricane ask more specifically about what was or what would be most critical about their technology use, and then ask generally about technology-related concerns.

C.1.3.1 Questions deployed at the start of hurricane season

Here we're going to ask a little more about your experience using technology during the disaster that affected you or your community. When answering these questions, please be as specific as possible!

Q1 How did your use of technology change in the recovery period after the disaster? [free response]

Q2 For example, what new apps or technologies did you use? What apps or technologies did you stop using? [free response]

Q3 Did you or anyone you know encounter any scams directed at people recovering from a natural disaster, or any other security and privacy issues?

Q4 If so, please tell us briefly about them. [free response]

Q5 Did you lose power, internet, or cellular service for an extended period of time? [yes, no]

Q6 If you had any issues with the questions in this section, please let us know here

C.1.3.2 Questions deployed during or immediately after a hurricane

Q7 How did your technology use change from normal during this extreme weather, if at all? Please be specific / detailed. [free response]

Q8 Did you use your phone / computer / tablet at all during this extreme weather? [yes, no]

`If the participant used technology during the storm, display the following three questions`

Q9 What did your phone / computer / tablet provide that was *most critical / important* **during** the situation?

Q10 What did your phone / computer / tablet provide that was *most critical / important* **in preparation** for the situation?

Q11 How do you think your experience would have changed if you hadn't been able to use your devices?

`If the participant did not use technology during the storm, display the following two questions.`

Q13 Why didn't you use your phone / computer / tablet?

Q14 How do you think your experience would have changed if you had used your devices?

`Display the following questions about concerns to all participants.`

`For participants currently experiencing a storm:`

Q15 What are your biggest technology- or internet-related concerns right now, if you have any?

`For participants who recently experienced a storm, display the following 3 questions:`

Q16 What were your biggest concerns during the situation?

Q17 What were your biggest technology- or internet-related concerns during the situation, if you had any?

Q18 What are your biggest technology- or internet-related concerns right now, if you have any?

C.1.4 Demographics

It is important that we understand the skew of our study sample, so this section asks for your demographic information. We have done our best to not ask unnecessarily invasive questions. However, we would like to remind you that all questions in this survey are optional and that you are not required to share any of this information with us. Q1 What is your age? [free response]

Q2 What is the highest level of school you have completed or the highest degree you have received?

- Less than high school degree
- High school graduate (high school diploma or equivalent including GED)
- Some college but no degree
- Associate degree in college (2-year)
- Bachelor's degree in college (4-year)
- Master's degree
- Doctoral degree
- Professional degree (JD, MD)

Q3 Choose one or more races or ethnicities that best fit your identity by checking all that apply. You can also (or instead) self-describe in the next question.

- American Indian or Alaska Native
- Asian
- Black or African American
- Hispanic, Latinx, or Spanish
- Native Hawaiian or Pacific Islander
- Middle Eastern
- South Asian

- South East Asian
- White

Q4 If you prefer to self-describe your race and ethnicity instead of or in addition to using the checkboxes above, please do so here. [free response]

Q5 What is your gender? Check all that apply.

- Woman
- Man
- Non-binary
- Prefer to self describe: [free form]

Q6 Information about income is very important to understand. Please indicate the answer that includes your entire household income in 2020 before taxes.

- Less than $10,000
- $10,000 - $19,000
- $20,000 - $29,000
- $30,000 - $39,000
- $40,000 - $49,000
- $50,000 - $59,000
- $60,000 - $69,000
- $70,000 - $79,000
- $80,000 - $89,000
- $90,000 - $09,000
- $100,000 - $149,000
- $150,000 or more

Q7 Do you think of yourself as closer to the Republican or Democratic party?

- Republican
- Democratic

Q8 What is the name of the town or city in which you live? [free response]

If you are not comfortable giving this, you can give the name of a nearby large city or town, or skip this question.

Q9 What is your zip code? [free response]

Q10 For how many years have you lived in your area? [free response]

Q11 If the above questions did not fit your identity, or if there is anything else you think we should know about you, demographically, please write it here. [free response]

Q12 If you had any issues with the questions in this section, please let us know here [free response]

C.1.5 Storm context module

`One of the following was displayed, as appropriate:`

- You indicated that you are experiencing a hurricane or tropical storm (or related weather).
- You indicated that you are expecting a storm or other extreme weather in the next 48 hours or so, or that you were expecting a storm that did not occur.

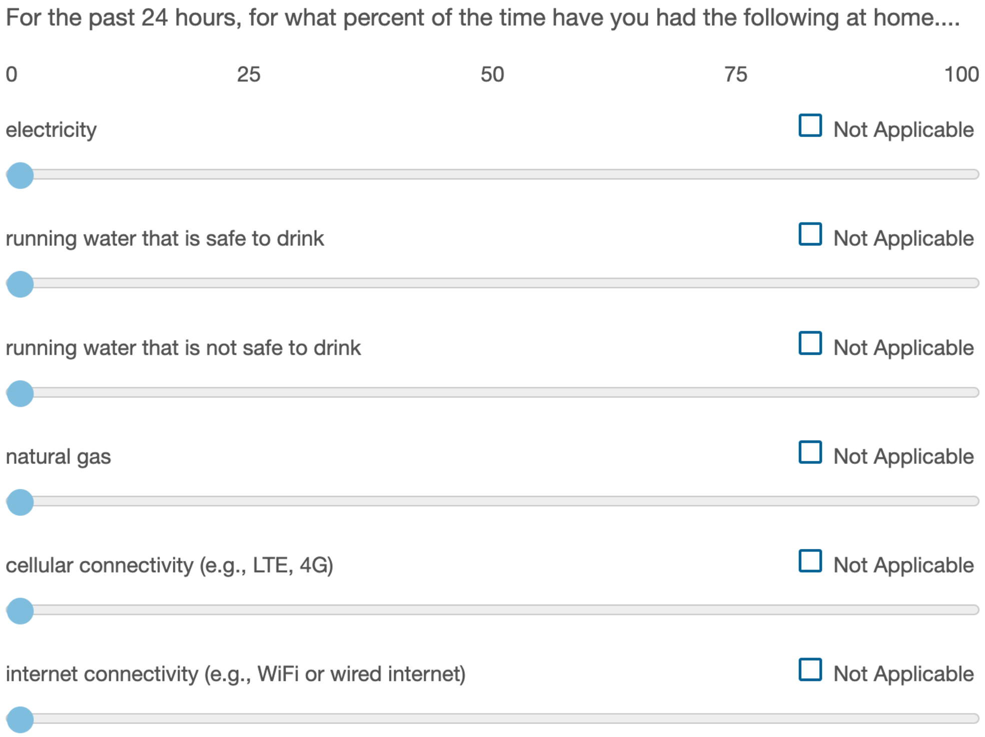
`During a storm, the following question was displayed:`

Q1 Briefly, what's going on? Please write at least one sentence, and feel free to write more. [free response]

`If participants that they were or had been expecting a storm, the following question was displayed:`

Q2 What type of weather do/did you expect?

`For surveys deployed after a storm, the following two questions were displayed instead:`



For the past 24 hours, for what percent of the time have you had the following at home....

0 25 50 75 100

electricity □ Not Applicable

running water that is safe to drink □ Not Applicable

running water that is not safe to drink □ Not Applicable

natural gas □ Not Applicable

cellular connectivity (e.g., LTE, 4G) □ Not Applicable

internet connectivity (e.g., WiFi or wired internet) □ Not Applicable

Figure C.3: Participants indicated the availability of certain common utilities at home during the storm using the sliders pictured.

Q3 Please briefly describe your experience of the storm. Was there extreme weather and, if so, what happened? What did you and your household experience? [free response]

Q4 How long did it last? [free response]

`The following questions were modified to include the correct tense based on whether the participant was currently experiencing a storm or had recently experienced a storm.`

Q5 How much has the storm interrupted your daily routine? [None, a little, a moderate amount, a lot, a great deal]

Q6 For the past 24 hours, for what percent of the time have you had the following at home....

`Participants were shown slider scales from 0-100 for each utility, as well` as a ‘not applicable’ button, as show in Figure C.3

Q7 In what ways has the extreme weather interrupted your daily routine? What do you want to do but are unable to? [free response]

Q8 In general, what do you expect will happen in the next 24 hours? [free response]

Q9 In general, what do you expect will happen in the next 7 days? [free response]

Q10 What are your biggest concerns currently? [free response]

C.1.6 Technology use during the storm module

This section was mostly comprised of two tables that asked participants to estimate how much time they spent on a category of activity like ‘social media’ in the past 24 hours. These two tables are shown in Figures C.4 and C.5

For participants who were currently experiencing a hurricane:

Q1 Please estimate the number of minutes you spent on each activity in the past 24 hours.

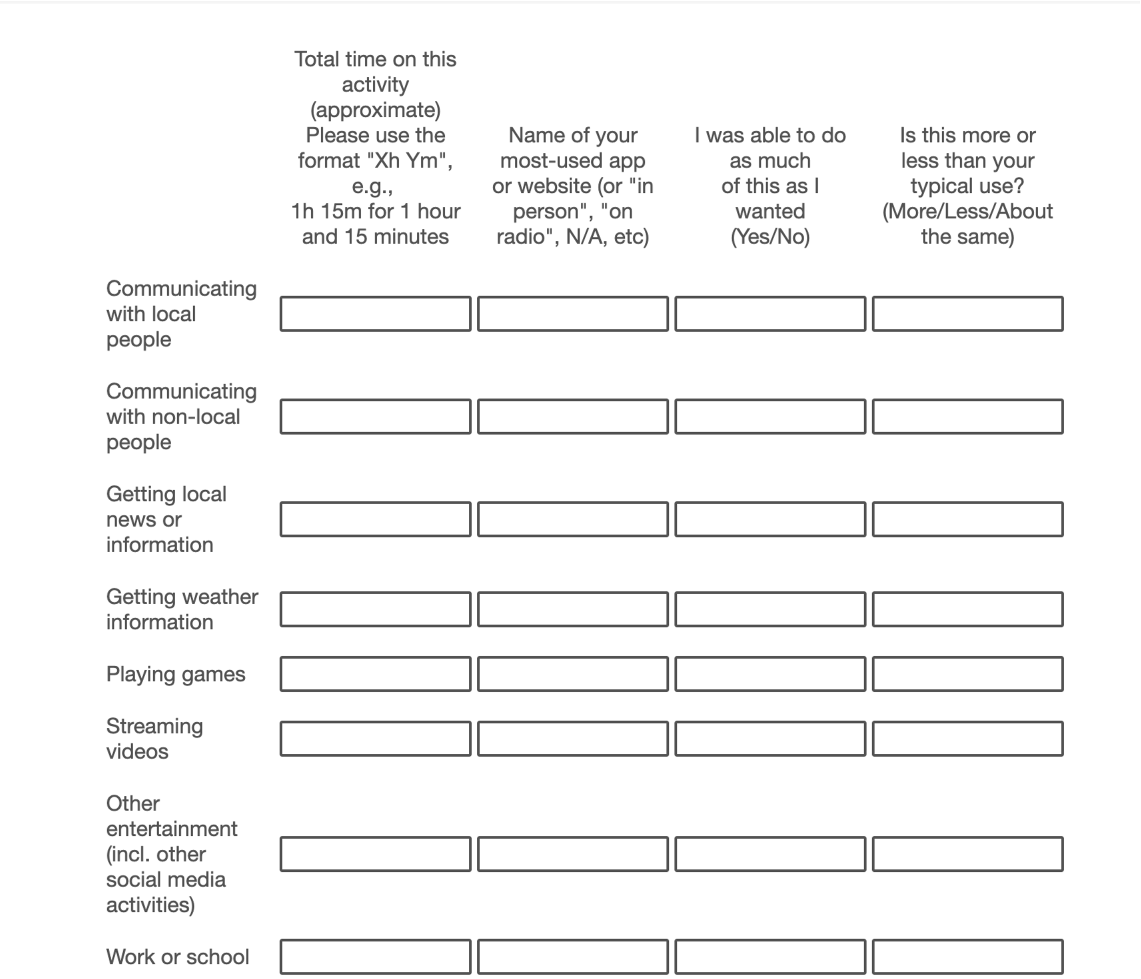
For participants who had recently experienced a hurricane:

Q2 Please estimate the number of minutes you spent on each activity in a typical 24 hours during the storm.

Participants were presented with an 8x4 grid of boxes to fill in. The columns were:

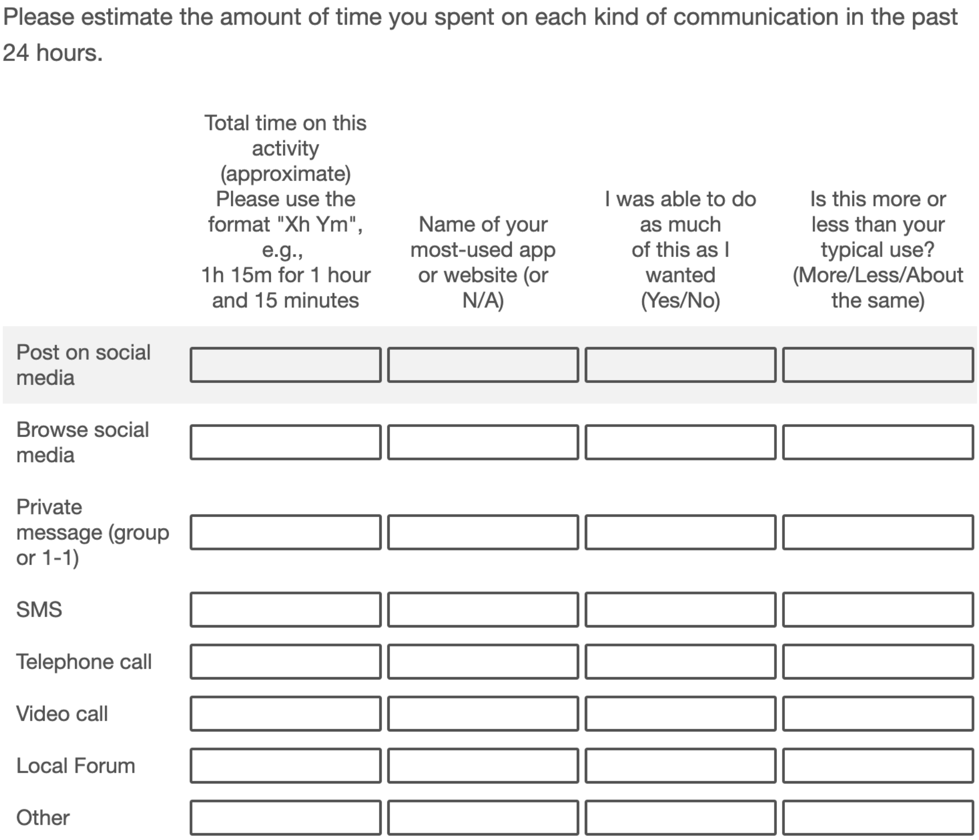
- Total time spent on this activity (Approximate). Please use the format “Xh Ym”, e.g., 1h 15m for 1 hour and 15 minutes.
- Name of your most used app or website (or N/A)
- I was able to do as much of this as I wanted (Yes/No)
- Is this more or less than your typical use? (More/Less/About the same)

The rows were:



	Total time on this activity (approximate) Please use the format "Xh Ym", e.g., 1h 15m for 1 hour and 15 minutes	Name of your most-used app or website (or "in person", "on radio", N/A, etc)	I was able to do as much of this as I wanted (Yes/No)	Is this more or less than your typical use? (More/Less/About the same)
Communicating with local people				
Communicating with non-local people				
Getting local news or information				
Getting weather information				
Playing games				
Streaming videos				
Other entertainment (incl. other social media activities)				
Work or school				

Figure C.4: Tech use table: high level task



Please estimate the amount of time you spent on each kind of communication in the past 24 hours.

	Total time on this activity (approximate) Please use the format "Xh Ym", e.g., 1h 15m for 1 hour and 15 minutes	Name of your most-used app or website (or N/A)	I was able to do as much of this as I wanted (Yes/No)	Is this more or less than your typical use? (More/Less/About the same)
Post on social media				
Browse social media				
Private message (group or 1-1)				
SMS				
Telephone call				
Video call				
Local Forum				
Other				

Figure C.5: Tech use table: type of technology used

- Communicating with local people
- Communicating with non-local people
- Getting local news or information
- Getting weather information
- Playing games
- Streaming videos
- Other entertainment (incl. other social media activities)
- Work or school

Q3 For any of the above activities that you were not able to do as much as you wanted: why not? [free response]

`For participants who were currently experiencing a hurricane:`

Q4 Please estimate the amount of time you spent on each kind of communication in the past 24 hours.

`For participants who had recently experienced a hurricane:`

Q5 Please estimate the number of minutes you spent on each kind of communication in a typical 24 hours during the storm.

`Participants were presented with an 8x4 grid of boxes to fill in. The columns were the same as the above. The rows were:`

- Post on social media
- Browse social media
- Private message (group or 1-1)
- SMS
- Telephone call
- Video call
- Local Forum

- Other

Q6 For any of the above activities that you were not able to do as much as you wanted: why not? [free response]

C.1.7 Module: recent InfoSec issues

In the this section, we're going to ask about some **things that you might have experienced in the past week**. In both categories (information security and device access), we have given several options for issues you might have experienced. Please do not be limited by these options; if you have experienced a different issue, however YOU define "issue" or "problem," we would like to hear about it! Check whatever fits you best, and please explain in the text boxes provided in the next question.

Q1 Information security:

- I experienced a scam, identity theft, stolen financial information (or attempts)
- My password(s) was/were stolen
- I was locked out of an account
- I encountered misinformation
- Another issue related to computer or information security or privacy

`If any of the previous choices are selected, display the following one question:`

Q2 You indicated that you experienced some sort of computer or information security or privacy issue. Please write a sentence or two about what happened. [free response]

Q3 Device Access:

- I got a new phone, tablet, or computer
- I got a new smarthome device (e.g., Alex, WiFi-enabled lightbulbs, Ring camera, etc)
- Another change in access to technology

`If any of the previous choices are selected, display the following one question:`

Q4 You indicated that you gained or lost (or got rid of) a piece of technology. Please us briefly what happened: what kind of device did you either gain or lost, and why?

`If either of the second two choices are selected, also display the following one question:`

Q5 If there is anything in particular you did with your new device(s) to prepare for a weather-related emergency, please explain here and be as specific as possible. [free response]

C.1.8 Module: Disaster kit usage and reflection

C.1.8.1 Questions deployed in the current hurricane survey

`These questions focus on changes to preparation`

We would like to learn about how you're using the items in your disaster kit. Please use the space below to list the items you've used from your kit.

Q1 Is there anything that you wish you had in your kit?

Q2 In the past week, have you changed anything about your disaster preparation?

- Yes, I have added items to my kit
- Yes, I have removed items from my kit
- Yes, I did something else (e.g., speaking with insurance, taking photos, etc)
- No changes

`If ‘‘Yes, I have added items to my kit’’ is selected, display the following questions:`

Please tell us a little about the changes you made to your disaster preparation....

Q3 What did you add? Why?

Q4 Who or what caused this addition? How did you hear about this item, or hear that it should be in your disaster kit?

`If ‘‘Yes, I have removed items from my kit’’ is selected, display the following questions:`

Please tell us a little about the changes you made to your disaster preparation....

Q5 What did you remove? Why?

Q6 Who or what caused this removal? How did you come to decide to remove this item?

`If ‘‘Yes, I did something else’’ is selected, display the following questions:`

Please tell us a little about the changes you made to your disaster preparation....

Q7 What were the changes you made? Why?

Q8 Who or what caused these changes? How did you hear about these changes, or learn that these changes would be useful to you?

C.1.8.2 Questions deployed in the post-hurricane survey

Q9 What items from your disaster preparation kit did you use, if any? [free response]

Q10 Consider your preparation. Is there anything you will change in the future? [free response]

For the next two questions, think about any digital or technical preparations you made – for example, maybe you took pictures of important documents, made backups, made copies of passwords, set up specific smart home rules, etc.

Q11 Which of these were useful? [free response]

Q12 Which do you expect will be useful in the future? (feel free to consider hypothetical or unlikely scenarios). [free response]

Q13 If you could invent a magic item or a magic solution to make extreme weather less impactful on you and your community, what would it be? Don’t consider cost or what is “possible” with technology or infrastructure. [free response]

Q14 Which of the following applied to you during the storm:

- I used the food or water in my disaster kit

- I used the supplies in my disaster kit to make or fix my shelter
- I used my emergency supply of power or light (e.g., candles, flashlights generator, etc)
- I used my supply of medical or hygiene equipment
- I used the extra currency in my disaster kit
- I used the weapons in my disaster kit
- I used the plans I made with others in my community
- I used my preparation of paper documents (e.g., I saved paper documents somewhere and referenced the documents, took them with me when I evacuated, etc)
- I used my preparation of digital documents (e.g., I saved documents digitally somehow and referenced the documents, used them to get a replacement paper document, etc)
- I used apps I downloaded specifically for the storm
- I used my external smartphone batteries
- I used my alternate communication methods

`Based on which of the options above were selected, the appropriate free response questions were displayed below:`

Q15 You said that you used the paper documents that you had prepared before the storm. Please write a sentence or two about why you had to use them and what you did with them. [free response]

Q16 You said you used the digital documents that you had prepared before the storm. Please write a sentence or two about why you had to use them and what you did with them. [free response]

Q17 You said you used apps you downloaded specifically for the storm. What apps? What did you use them for? [free response]

Q18 You said you used external smartphone batteries. For how long did you rely on the external smartphone batteries? What did you do with your phone while you were relying on the batteries? [free response]

Q19 You said you used alternate communication methods. What did you use? Why? Did it work? [free response]

C.2 Hurricane survey flows

The following subsections give the consent text, the survey modules, and any extra questions that appeared in the surveys. We also include the recruitment messages for the during-hurricane survey, since we sent individual messages to participants. See Figure 5.2 for a visual representation of how the modules appeared in each survey.

C.2.1 Retrospective Survey

C.2.1.1 Screening

This is a screening survey for a survey by researchers at the University of Washington, in Seattle, Washington, USA, and the Max Planck Institute for Security and Privacy in Bochum, Germany. The University of Washington's Human Subjects Division reviewed our study, and determined that it was exempt from federal human subjects regulation. We do not expect that this survey will put you at any risk for harm, and you don't have to answer any question that makes you uncomfortable; however, if you do not answer all the questions, you will not be eligible for our future survey.

We expect this screening survey will take less than a minute to complete. If you have any questions, you may email Lucy Simko at `study-specific-gmail`. If you are eligible, we may send you another survey on Prolific. Thank you for taking our screening survey!

Are you at least 18 years old? [no, yes]

Do you live in an area that is affected by hurricanes or tropical storms? [no, yes]

What is your zip code? [free response]

What is your Prolific ID? [free response]

C.2.1.2 Survey

`Before any major hurricanes had hit the US`

This is a survey about natural disasters and technology use by researchers at the University of Washington, in Seattle, Washington, USA, and the Max Planck Institute for Security and Privacy in Bochum, Germany. The University of Washington's Human Subjects Division reviewed our study, and determined that it was exempt from federal human subjects regulation. We do not expect that this survey will put you at any risk for harm, and you don't have to answer any question that makes you uncomfortable. In order to participate, you must be at least 18 years old, live in an area affected by hurricanes or tropical storms, and be comfortable completing the survey in English.

We expect this survey will take about 20 minutes to complete. This survey asks about your experience using technology during a natural disaster (for example: hurricane, flooding, earthquake, tornado, extreme cold, etc). Though the survey focuses primarily on your experience with technology before, during, and after such a disaster, we will ask some questions about your experience during the disaster itself. Thus, it is possible that some questions will evoke unpleasant or traumatic memories for you. Though we appreciate your full answers, your well-being comes first, and you are welcome to skip any questions that you do not want to answer. You may also withdraw from the study at any time, but if you do not reach the end of the study you will not recieve the completion code, so you will not be paid.

Based on your responses, we may ask you to complete other surveys some time in the next three months. However, you are not agreeing to do future surveys simply by completing this survey today.

If you have any questions about this survey, you may email Lucy Simko at `survey-specific-gmail` or message us on Prolific. To start, please answer the two questions below...

Are you at least 18 years old? [no, yes]

Do you live in an area that is affected by hurricanes or tropical storms? [no, yes]

What is your prolific ID? [free response]

Preparation module *(Section C.1.1)*

App module *with the following question to filter out people who had never experienced a disaster (Section C.1.2)*

In the past 10 years, have you experienced a disaster that had a considerable impact on you or your community?

A disaster could be a natural disaster, like a hurricane, or it could be an manmade accident, or it could be something like a terrorist attack.

Considerable impact is however you personally define it; there is no wrong definition. The impact could be financial, physical, emotional, or something else.

If you are not sure if something "counts," we recommend saying yes and not answering questions if they do not apply. [yes, no]

`If yes, the following free-response question is displayed:`

Please briefly write a sentence or two about what happened.

Tech reflection module *(Section C.1.3)*

C.2.2 During-hurricane survey

C.2.2.1 Screening Survey

This is a screening survey for a survey by researchers at the University of Washington, in Seattle, Washington, USA, and the Max Planck Institute for Security and Privacy in Bochum, Germany. The University of Washington's Human Subjects Division reviewed our study, and determined that it was exempt from federal human subjects regulation. We do not expect that this survey will put you at any risk for harm, and you don't have to answer any question that makes you uncomfortable; however, if you do not answer all the questions, you will not be eligible for our future survey.

We expect this screening survey will take less than a minute to complete. If you have any questions, you may email Lucy Simko at `study-specific-gmail`. If you are eligible, we may send you another survey on Prolific. Thank you for taking our screening survey!

Are you at least 18 years old? [no, yes]

Are you currently being affected by `[hurricane name]`?

- Yes, I evacuated
- Yes, I am sheltering in place
- Yes, other: [free response box]

What is your zipcode? [free response]

What is your Prolific ID? [free response]

C.2.2.2 Survey

C.2.3 Recruitment message for the during-hurricane survey

`We sent the following text as a direct message on Prolific to participants who were eligible for the during-hurricane survey.`

Hi!

You are eligible for our next survey, which is about technology use during a hurricane. Please find it here: [qualtrics url]

If you chose to do the next survey, we will bonus you $12. We expect it will take you about 40 minutes. We understand that 40 minutes is a long time and you may lose power or internet; just do your best – we'll pay you for any portion that you complete (i.e., if you complete about half, we'll pay $6) :)

(If you would prefer, we can release this as a formal study through the interface; we're just doing these one at a time so we thought it would be easier to message you directly).

Let us know if you have any questions and please stay safe! Best,

[two researchers names]

This is a survey about natural disasters and technology use by researchers at the University of Washington, in Seattle, Washington, USA, and the Max Planck Institute for Security and Privacy in Bochum, Germany. The University of Washington's Human Subjects Division reviewed our study, and determined that it was exempt from federal human subjects regulation. We do not expect that this survey will put you at any risk for harm, and you don't have to answer any question that makes you uncomfortable. In order to participate, you must be at least 18 years old, live in an area affected by hurricanes or tropical storms, and be comfortable completing the survey in English.

We expect this survey will take about 40 minutes to complete. This survey asks about your experience using technology during a hurricane or tropical storm that may be happening right now. We understand that 40 minutes may be a long time, or that you may lose connection. Just do your best and stay safe!

Though the survey focuses primarily on your experience with technology before, during, and after such a disaster, we will ask some questions about your experience during the disaster itself. Thus, it is possible that some questions will evoke unpleasant or traumatic memories for you. Though we appreciate your full answers, your well-being comes first, and you are welcome to skip any questions that you do not want to answer. You may also withdraw from the study at any time, but if you do not reach the end of the study you will not recieve the completion code, so you will not be paid. If you have any questions about this survey, you may email Lucy Simko at *study-specific-gmail* or message us on Prolific. To start, please answer the two questions below ...

Are you at least 18 years old? [yes, no]

Please check the box below that most accurately reflects your current situation:

- I am currently experiencing a hurricane or tropical storm (including flooding, heavy rain, high wind, etc) or I evacuated for one
- I expect to experience a hurricane or tropical storm within 48 hours (i.e., I am under a hurricane or tropical storm watch or warning)

What is your Prolific ID? [free response]

Preparation module*, modified tense as appropriate (Section C.1.1)*

App module *(no filter question) (Section C.1.2)*

Storm context module *(Section C.1.5)*

Tech use during storm module *(Section C.1.6)*

Technology reflection module *(Section C.1.3)*

Infosec issues module *(Section C.1.7)*

Demographics module *(Section C.1.4)*

C.2.4 Post-Ida survey

C.2.4.1 Screening Survey

This is a screening survey for a survey by researchers at the University of Washington, in Seattle, Washington, USA, and the Max Planck Institute for Security and Privacy in Bochum, Germany. The University of Washington's Human Subjects Division reviewed our study, and determined that it was exempt from federal human subjects regulation. We do not expect that this survey will put you at any risk for harm, and you don't have to answer any question that makes you uncomfortable; however, if you do not answer all the questions, you will not be eligible for our future survey.

We expect this screening survey will take less than a minute to complete. If you have any questions, you may email Lucy Simko at `study-specific-gmail`. If you are eligible, we may send you another survey on Prolific. Thank you for taking our screening survey!

Are you at least 18 years old? [no, yes]

Did you experience hurricane Ida recently?

- No
- Yes, I was severely affected
- Yes, I was moderately affected
- Yes, I was somewhat / slightly affected

What is your zipcode? [free response]

What is your Prolific ID? [free response]

C.2.4.2 Survey

This is a survey about natural disasters and technology use by researchers at the University of Washington, in Seattle, Washington, USA, and the Max Planck Institute for Security and Privacy in Bochum, Germany. The University of Washington's Human Subjects Division reviewed our study, and determined that it was exempt from federal human subjects regulation. We do not expect that this survey will put you at any risk for harm, and you don't have to answer any question that makes you uncomfortable. In order to participate, you must be at least 18 years old, live in an area affected by hurricanes or tropical storms, and be comfortable completing the survey in English.

We expect this survey will take about 15 minutes to complete. This survey asks about your experience using technology during a hurricane or tropical storm that happened 1-2 weeks ago.

Though the survey focuses primarily on your experience with technology before, during, and after such a disaster, we will ask some questions about your experience during the disaster itself. Thus, it is possible that some questions will evoke unpleasant or traumatic memories for you. Though we appreciate your full answers, your well-being comes first, and you are welcome to skip any questions that you do not want to answer. You may also withdraw from the study at any time, but if you do not reach the end of the study you will not recieve the completion code, you will not be paid. If you have any questions about this survey, you may email Lucy Simko at `study-specific-gmail` or message us on Prolific. To start, please answer the question below ...

Are you at least 18 years old? [yes, no]

What is your Prolific ID numbers? [free response]

Based on a screening survey you filled out recently, we understand that you recently experienced `[Name of recent storm, e.g., ‘‘Hurricane / Tropical Storm Ida’’]`.

Context module *(Section C.1.5)*

The next questions ask you about your disaster preparation and technology use during the storm that you just experienced. We appreciate your thoughtful, detailed, and specific answers to these questions.

Technology reflection module *(Section C.1.3)*

Disaster kit usage module *(Section C.1.8)*

Tech use during storm module *(Section C.1.6)*

Infosec issues module *(Section C.1.7)*

C.3 Codebook

Category	**Code**	**Definition or example**
Needs	Find resources	Finding gas, groceries, batteries
	Emotional stability & psych. safety	e.g., don't look at the news because it makes you scared
	Entertainment	"pass time," entertainment, stave off boredom
	Evacuation routes	Find the safest route out of disaster
	Be informed	Stay up to date w/info, know about family, etc
	Communicate	Talk to friends and family
	Communicate – Safety check	Tell ppl you are safe. Includes passive safety checks
	Financial stability	School/job impacted or other financial impact.
	Physical safety	General safety & emergency info & alerts.
	Get help in an emergency	e.g., use ICE app, send emergency contacts location
Information needs: *Quality of info*	Accurate & trustworthy	information is correct and they trust it
	Volume	e.g., nothing important missing. Includes detail.
	Timeliness	News is up-to-date / current
Information needs: *Type of info*	Weather info	Radar, forecasts, etc
	Assistance	Find / give storm recovery help
	Info about community	See the extent of the damage, get local news, locals advisories. Does *not* incl. emergency alerts (use physical safety instead).
	Info about the world	Keep up with the news in general (not local)
	Learn what to do	Learn what they should do, individually, to recover from, ride out, or prepare for the storm. *Not* learn where to get resources, find evac routes, or generally stay informed.

Table C.1: Our codebook (part I).

Category	**Code**	**Definition or example**
New strategies: *Keep phone running*	Ration electricity	Decreasing use because they're relying on another electricity source, don't use X app because it drains the battery. Can infer if they're talking about a power outage and they say they used their phone less.
	Alternative charging methods	Phone bank, neighbor's house, etc
	Phone settings	Lower brightness, low power mode, etc
New strategies: *Keep in touch*	Advance check-in times	Plan to check in anticipation of infrastructure being down
	Visit in person	Went to check on friends/family
	Offline communication	use apps that work offline or they believe work offline
	Rely on people not as affected by the storm	e.g., neighbors, friends
	Manually relay messages	Used messaging apps or phone calls to spread info about others / between others
	VoIP apps	Call over wifi instead of the tele phone
	Telephone	Used the telephone
New strategies: *Connectivity*	Ration time online	limit time using connectivity
	Travel locally	Go somewhere that has connectivity
	Use mobile data	Use mobile data instead of internet
	Radio	Use a one-way or two-way radio
	Mobile hotspot	Connect to the internet using a mobile hotspot
New strategies: *Get/share info*	Crowdsourcing / digital volunteerism	look for info on social media, share info on social media
New strategies: *other*	Living arrangement change	e.g., candles. includes ”no tech”

Table C.2: Our codebook (part II).

Category	**Code**	**Definition or example**
Tech use during storm	In-case-of-emergency	Mention of a specific app in a free response question or it's abundantly clear what app or technology their response refers to
	Text communication	
	Audio / video comm.	
	Weather	
	Social media	
	Local news	
	National news	
	Unk. communication	Communication tech but unclear what kind
	Other news	News but unclear whether local or national
	Other app	
Storm context: *Storm*	Debby	Name of hurricane they experienced
	Florence	
	Harvey	
	Ike	
	Irma	
	Matthew	
	Sally	
	Unnamed hurricane	
	Non-hurricane	Some other natural disaster (specific)
Storm context: *Outages*	Electricity	Power outage — may have generator or batteries
	Cellular	Cellular service outage
	Internet	Internet outage (WiFi or terrestrial internet)
	Unspecified loss of connectivity	Some connectivity outage, not specified (cell / internet)
	Unspecified outage	Some outage, not specified
	Concerned about outage	Worried that an outage will happen
Infosec issues	[no subcode]	Any mention of misinformation, scams, or anything *they* considered security and/or privacy

Table C.3: Our codebook (part III).