Advancing Digital Safety for High-Risk Communities

by

Allison McDonald

A dissertation submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
(Computer Science and Engineering)
in The University of Michigan
2022

Doctoral Committee:

Professor J. Alex Halderman, Co-Chair
Assistant Professor Florian Schaub, Co-Chair
Associate Professor Nicola Dell
Professor H. V. Jagadish
Professor Kentaro Toyama

Allison McDonald
amcdon@umich.edu
ORCID iD: 0000-0001-7477-6782

ACKNOWLEDGEMENTS

I would like to first thank my advisors, Florian Schaub and Alex Halderman, for their years of support and guidance. I have learned a great deal from you both about how to conduct meaningful scholarship, and how to shepherd that work into the world to make it as impactful as possible. I am also grateful to my committee members, Kentaro Toyama, Nicola Dell, and H V Jagadish, who have not only strengthened my work here but have been models for the scholar I want to be.

I have been incredibly fortunate to work in a collaborative environment with many people who have challenged my thinking, supported my growth, and often become dear friends. I am grateful to my collaborators, labmates, and friends: Mohamed Abbadi, David Adrian, Tanisha Afnan, Catherine Barwulor, Janet Chen, Sylvia Darling, Zakir Durumeric, Roya Ensafi, Sai Gouravajhala, Tamy Guberek, Vaughn Hamilton, Peter Honeyman, Jane Im, Fahad Kamran, Deepak Kumar, Kevin Loughlin, Allan Martell, Michelle Mazurek, Henry Meng, Ariana Mirian, Susan O'Connor, Justin Petelka, Elissa Redmiles, Tom Ristenpart, Kat Roemmich, Kevin Roundy, Will Scott, Megan Shearer, Steve Sprecher, Drew Springall, Carlo Sugatan, Kaiwen Sun, Acar Tamersoy, Emily Tseng, Wes Weimer, Eric Wustrow.

I specially want to thank Matthew Bernhard, Benjamin VanderSloot, Reethika Ramesh, Ramakrishnan Sundara Raman, Yixin Zou, Abraham Mhaidli for their friendship, camaraderie, kindness, support, and humor throughout the past six years. I can't imagine having done this without each of you.

And most importantly, I want share my love and gratitude for the support I've been given by my mom, my sister Emily, and my partner Ritchie. Thank you for indulging my

decision to stay a student for over a decade (!), and especially for the care you've all shown me in the last six years when I needed it most.

TABLE OF CONTENTS

CHAPTER

LIST OF FIGURES

Figure

LIST OF TABLES

Table

LIST OF APPENDICES

Appendix

ABSTRACT

Privacy and security tools and strategies are not equally effective for everyone—many high-risk communities, such as sex workers, undocumented immigrants, and survivors of intimate partner violence, face security, privacy, and safety risks that are not well addressed by current solutions. This dissertation explores how technology and vulnerability intersect to create differences in access and digital safety for different high-risk populations, and demonstrates the strengths of investigating these issues using a mix of both in-depth qualitative and large-scale quantitative methods.

By exploring the particular privacy and security needs of undocumented immigrants in the United States and sex workers in Europe, I first discuss the primary safety goals and the barriers to these goals for two specific high-risk populations. Both studies revealed factors, both human and technical, that made privacy and security difficult. Many of the tools and platforms our participants relied on were not built with high-risk users in mind, and failed to provide sufficient protection or controls to meet their specific safety needs. I next examine two particular technologies that lead to privacy and access problems: the collection and use of phone numbers as account identifiers, and the application of geoblocking by companies to deny entire countries access to their websites. In both cases, I propose moderate changes to features that could make a significant impact on minimizing harms for vulnerable users. Finally, I present a comprehensive framework that connects privacy harms, personal and community risk factors, and the technical mechanisms that lead risk factors to result in harm. This framework identifies themes for how a broad set of populations are impacted by tech and policy design choices, and enables us to identify patterns in harm across multiple communities.

Thesis statement. High-risk populations, who have a heightened need for effective privacy and security tools, face unique privacy challenges. Technology can reinforce and perpetuate marginalization through policies and technical features that amplify the privacy and security risks of vulnerable groups.

CHAPTER I

Introduction

The Internet promises unprecedented access to information, community, and financial opportunity, while simultaneously offering a new medium for government and corporate surveillance [399], State censorship [397], and harassment and other abuse [125, 360]. Computer privacy and security as a field seeks to provide the means for people to defend against these intrusions, from buttressing core Internet infrastructure with encryption [141], building bespoke privacy and anonymity tools like Tor [120] and Signal [338], to understanding and addressing where users' privacy expectations and reality diverge (e.g., [3, 398, 96]).

Despite the significant strides we've made in building privacy and security into the Internet, however, not all people have the same access to safe participation in digital spaces [247, 341]. In particular, marginalized and otherwise high-risk populations often face greater barriers to access, as well as heightened threats and outsized consequences of privacy invasions and security failures. For the purposes of this dissertation, a "high-risk population" means those groups who face an increased *likelihood* of privacy harm as well as those who face increased *consequences* should they experience some privacy intrusion or security failure.

There are several reasons the study of high-risk populations in particular is critical for effectively addressing privacy and security issues. First, the users in underserved and high-risk communities are often going to be users who can teach us from experience how security tools and protective strategies succeed or fail for highly-motivated users who depend on them. Second, by identifying the previously overlooked needs of marginalized and otherwise vulnerable communities, we can more effectively develop a safer, more accessible, and more equitable digital future. Finally, by improving the safety and accessibility of the Internet for high-risk users, we will increase the baseline level of security and privacy for all users, across the risk spectrum. As I will discuss in Chapters III and VI, a person's digital privacy and security goals may be diverse and depend on other, broader needs like being able to access online communities and ensure financial security. For this reason, I will use the term "safety" to broadly encompass these interlocking needs, which include digital privacy and security.

There are many factors that lead to someone needing greater protection online. For example, a person may face a particular adversary, such as an abusive ex-partner or a repressive regime seeking to suppress their speech, which means that maintaining privacy and security takes excessive effort and is more likely to fail over time [249, 245]. If a person has a marginalized identity, like a stigmatized health condition or a minority religious belief, this could put them at higher risk of discrimination and harassment when disclosed [341, 6]. In addition to personal or social factors that may make a population more vulnerable, the digital tools and platforms that people use may themselves magnify risk. For example, audience control and privacy settings on social media platforms are not always sufficient to prevent unwanted disclosures [238, 246, 388]. Facebook's People You May Know feature, which suggests other accounts to connect with based on information collected about a user, might proactively suggest a personal account to people one interacts with exclusively in a different context. For many people, this may be welcome, and at worst annoying. For others, it may be dangerous or violating: the tool has been shown to expose sex workers' legal names to clients [190] and reveal people's full names to other members of their Alcoholics Anonymous groups, against the tradition of the organization [221]. Platforms might increase offline risk as well—a person who associates their phone number with an account could have it subpoenaed by law enforcement and used to track them, as has been done by U.S. Immigration and Customs Enforcement seeking undocumented immigrants [343]. The global scale of many digital platforms also means these consequences manifest internationally; the exportation of American norms and laws, like the prohibition of sex work on major social media platforms [132, 40], even in countries where sex work is legal, or the banning of Iranian visitors to American websites through geoblocking [252], means that these policies have a global impact.

This dissertation explores how technology and vulnerability intersect to create disparate access to digital safety for different populations, and demonstrates the strengths of investigating these issues using a mix of both in-depth qualitative and large-scale quantitative methods. Specifically, my findings contribute to our understanding of how digital platforms and tools may perpetuate or uphold vulnerability by exploring the security and privacy risks and strategies of specific high-risk populations, as well as how specific technologies impact one's ability to stay safe. Using insights from these studies and a comprehensive literature review of privacy harms experienced by vulnerable populations, I then present a framework that synthesizes dimensions of risk and technical mechanisms that lead to harms, which provides an overview of how a broad set of populations are impacted by tech and policy design choices, and enables us to identify patterns in harm across multiple communities.

Here I will give a brief overview of each of chapters that follow. Finally, in Chapter VII, I discuss lessons learned and future directions for this work. While I've written the introduction and conclusion in the first person, I will use "we" when writing about specific projects to acknowledge the collaborative nature of the work.

1.1 Understanding Digital Vulnerability

I first explore **the role of vulnerability in people's understanding of digital risk and protective behaviors.** I present studies on the privacy and security needs and strategies of two communities with significant digital risk: undocumented immigrants and sex workers. While both communities face significant risk online from unwanted disclosure and surveillance, the salience of the risks resulted in very different threat models and strategies for safety. For sex workers, who heavily depend on the Internet to conduct their businesses, sources of risk were well known and many of our participants had highly developed protective strategies. For our undocumented participants, the significant offline risks of exposure to immigration enforcement largely had not translated to changing their online behavior. For both communities, when members did take measures to stay safe, some well-considered strategies were nonetheless difficult or impossible to achieve due to challenges with technology.

1.1.1 Technology, Risk and Privacy among Undocumented Immigrants

In Chapter II, I present a study in which we conducted 17 semi-structured interviews with undocumented immigrants in the U.S. Midwest on their technology use and risk perceptions [179]. Undocumented immigrants in the United States face risks of discrimination, surveillance, and deportation [271, 214, 372]. Our study was conducted in 2017, shortly after a U.S. election that sparked increased fears of deportation among immigrants [145]. For a population with significant risk and motivation to stay "under the radar," we sought to understand whether increasing risk both on- and offline translated to changes in the technology use, risk perceptions, and digital protective strategies of undocumented immigrants.

We find that, while our participants had highly-developed strategies for managing offline risks, this effort often did not translate to their online activities. Where concern existed, the benefits of the technology—like the ability to keep in touch with family in their country of origin—often outweighed the perceived risks. Nonetheless, our participants shared several sources of concern in their online activities, including visibility on social media, self-censorship on issues relating to immigration, and group privacy (for example, the ability of a digital support network to expose other members of the group as undocumented). From these concerns, we surface several ways that technology can be changed—sometimes in relatively minor ways, like obscuring phone numbers in large group chats—to substantially impact exposure risks and well-being for this community.

1.1.2 Safety in Digital Sex Work

In Chapter III, I present a study in which we conducted 29 interviews with European sex workers about their definitions of safety, their technical privacy and security needs, and the ways they manage risk, as well as data from a follow-up survey of 65 sex workers that allowed us to assess prevalence of common protective strategies [251]. As with undocumented immigrants, sex workers face risks of surveillance and exposure online. However, sex workers are increasingly conducting their business online [106, 327], and are thus dependent on digital tools to protect themselves from risks that had previously been strictly offline, like aggressive or obsessive clients and being unintentionally outed as a sex worker to friends and family. From a population with heightened consequences of failing to meet their digital privacy and security needs, and therefore with significant motivation to become proficient at digital safety, we can learn about how some existing tools and strategies work well, and how others create barriers to safety.

We found that our participants had broad and multifaceted conceptions of safety. Digital safety includes privacy and security, but also encompassed factors such as financial security, physical safety, and a need for respect. To meet these safety goals, sex workers face multiple challenges, including managing separate identities online to avoid being outed, carefully curating a work persona that is authentic yet hides personal details, e.g., via careful control of images that are on social media, and avoiding encounters with law enforcement. In some cases, these safety goals are difficult or impossible to achieve because platforms are not designed for users with multiple siloed identities. For example, platforms that track or connect users via identifiers that may be persistent across personas, like a phone number or credit card number, risk outing sex workers by algorithmically connecting their separate identities. The ability to do sex work safely online is also hindered by the enforcement of

American anti-sex-work laws and norms on globally-dominant platforms, cutting off access to community and resources even in regions where sex work is legal.

1.2 Technical Barriers to Safety & Access

I next investigate **how platform design and information policies can create barriers to safety and access** by focusing on two particular features: the use of a phone number as a digital user identifier and websites' decision to geoblock users based on their location. In both previous studies, instances of phone numbers being used as an account identifier created risks of unwanted exposure. Through a large qualitative elicitation survey, we catalog the ways that phone numbers create problems when used as identifiers. Though the most common issues were minor or temporary, some experiences like those leading to harassment and unwanted exposure could have significant consequences. Potentially harmful infrastructure is not, however, only deployed at a user-facing level. Geoblocking creates disparate access to information by blocking access to a website based on the geolocation of the visitor's IP address. We conducted a global measurement of geoblocking on popular websites and observed that geoblocking is common, though disproportionately impacts a handful of countries, especially those under U.S. sanctions and those already experiencing state censorship. In particular, this study demonstrates the potential of measurement work to surface differences in treatment at scale, as well as to surface where in the pipeline these discrepancies are being enforced.

1.2.1 Phone Numbers as a Case Study for Risky Design

As shown in the previous chapters, specific design choices can create privacy and security challenges for users with particular needs. In Chapter IV, we examine in detail one of the design decisions that we had observed creating challenges with identity management and exposure risks—the use of a phone number as an identifier on online platforms [253]. We conducted a qualitative elicitation survey with 195 participants, which allowed us to elucidate the specific harms such a decision creates across a broad swath of users.

Based on the experiences of our participants, we catalog the problems and consequences that arise when a phone number is used as an identifier. Although phone numbers are treated as persistent, unique, and consistently available, phone number instability and phone number recycling make phone numbers an unreliable identifier. Problems encompassed loss of access to accounts because the mobile network is not available, inconvenience from unwanted contact via phone, and unwanted interpersonal risk when a number is exposed on a platform to other users (e.g., on a dating site). Further, phone number recycling, a common challenge when one gets a new phone number, exacerbates these problems because two people become entangled with the same digital identifier. In light of the challenges phone numbers can pose to users, we discuss several possible mitigating steps for regulators, who should consider strategies for reducing phone number recycling, and companies, who should offer alternative modes of identification and authentication and avoid SMS-based multi-factor authentication.

1.2.2 Global Disparate Access to Content via Geoblocking

Harmful design choices do not belong exclusively to user-facing platforms. Companies involved in hosting and distributing web content can create or enable disparate impact on populations via the tools they provide to their customers. In Chapter V, we describe a large-scale Internet measurement study of *geoblocking*, or the server-side blocking of IP addresses—and thus users—by geolocation [252].

By leveraging the fact Content Distribution Networks (CDNs) offer template block pages to their many customers, we measure the availability of roughly 12,000 popular websites across 177 countries. We observed that IP addresses in different countries have remarkably different access to the Internet, with as many as 4.4% of websites blocking access in at least one country. In particular, we observed the impact of American export laws, which led to many American companies blocking all traffic from Sudan, Syria, Iran, and Cuba.

Finally, we worked with a large American CDN, Cloudflare, to observe how their clients use geoblocking features. We saw that many of their customers use these features liberally, and that when the feature was made available to free-tier customers, the number of sites blocking users by location went up significantly. Shortly after our study, Cloudflare restricted access to these features to enterprise customers, which immediately reduced the number of sites unavailable to users because of their location.

1.3 A Taxonomy of Risks and Mechanisms of Privacy Harm

Each high-risk population has a unique set of needs and constraints with respect to privacy, security, and safety. However, many of these needs overlap based on shared characteristics, similar adversaries, and shared desired outcomes of protective behavior. For example, although the consequences of exposure are different, both sex workers and undocumented immigrants have an identity they might want to hide—or selectively reveal—online. In both cases, unwanted exposure of this information, like through a social network's friend recommendation algorithm or by revealing networks of support groups, can be dangerous. By synthesizing risks of privacy harms across many high-risk populations, as well as the technical mechanisms that research suggests lead to these harms, we can better understand and anticipate these harms across populations and platforms.

Chapter VI proposes a framework that allows us to reason about risk and technology across populations. By combining the insights from the preceding chapters with a broader literature survey on digital privacy for high-risk populations, we distilled common dimensions of risk, identified how these risks relate to privacy harms, and characterized the technical mechanisms that enable these harms to occur online. The framework enables us to identify patterns of privacy harms across populations, reason about the most likely privacy harms of any high-risk population based on their risk factors, and identify which technical mechanisms can exacerbate these risk factors.

CHAPTER II

Technology, Risk and Privacy among Undocumented Immigrants[1]

Undocumented immigrants are those who have entered or remained in a country without authorization from the government. Like almost everyone else today, undocumented immigrants are users of information and communication technology (ICT). While ICTs have been found to support immigrants' integration in new contexts [84, 85, 105, 364], technology can also enable discrimination, harassment, and government surveillance, the latter potentially leading to devastating consequences such as detention, deportation, and family disruption [214]. For the estimated 11 million undocumented immigrants in the United States [295], these risks intensified during the 2016 U.S. presidential election, which inflamed anti-immigrant sentiment and threatened more aggressive immigration enforcement and anti-immigrant sentiment [212, 236].

Little is known about what role technology plays in the daily lives of undocumented immigrants and how it affects their vulnerability. Undocumented immigrants would be expected to have strong motivation to protect their privacy when using technology [100, 237, 352], but it is unclear how aware they are of ICT-related privacy and surveillance risks,

[1] This chapter is based on: Tamy Guberek, Allison McDonald, Sylvia Simioni, Abraham H. Mhaidli, Kentaro Toyama, and Florian Schaub. 2018. Keeping a Low Profile? Technology, Risk and Privacy among Undocumented Immigrants. In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18). [179]
This project was supported by the University of Michigan School of Information.

whether they adopt privacy-protective strategies, or how effective any such strategies are. Prior research on online privacy behavior of the general population suggests that, despite concerns, people often do not take protective action [186, 366].

To understand how undocumented immigrants navigate the benefits and risks of digital technology, we conducted semi-structured interviews with 17 Latinx[2] undocumented immigrants in an urban U.S. Midwest context. Undocumented immigrants from Latin America constitute the largest such group in the United States [295].

Our findings provide new insights on undocumented immigrants' technology use, as well as their understanding and attitudes toward digital security and privacy. To a great extent, our participants' behaviors with respect to security and privacy reflect that of the broader population — despite some concerns, they were neither particularly concerned about online privacy, nor did they take significant steps to protect it. This is surprising given the far greater threat that information disclosures have on their lives.

We identify a number of reasons for this: First, smartphones and social media are viewed to have indispensable benefits by our participants. Second, our participants have only a vague understanding of technology-related privacy and surveillance risks, making any potential consequences seem uncertain. Third, they tend to place significant trust in the major social media platforms. Fourth, participants feel that any information about them is readily available to government authorities, so they did not think *additional* exposure online would affect that risk.

Nonetheless, there were several ways in which our participants took protective measures and yet were unsure of their effectiveness or concerned about unwanted exposure. We surface that even minor design decisions, such as the use of phone numbers as account identifiers, can substantially affect the exposure risk of vulnerable communities.

These findings have further implications for the development of educational resources for immigrant communities; the design of transparency cues and privacy controls; and the

[2] Latinx is a gender-neutral term referring to both Latinos and Latinas.

design of ICTs in general.

2.1 Related Work

To situate our research, we describe related work on integration of undocumented immigrants, immigrants' technology use, and research on privacy and security concerns and behavior.

2.1.1 Undocumented Immigrants and Integration

Prior research has studied many challenges undocumented immigrants face [164], including cultural integration [42, 80], health [240, 283], and parenting [353]. Children of undocumented immigrants, even if they have legal status, struggle with identity, isolation, stress and anxiety [74, 163, 180], as well as reduced political integration [65].

One way undocumented immigrants avoid risks that come with their vulnerable legal status is to limit contact with authorities and institutions, even non-governmental ones offering heath care and social services [42, 80, 240]. They may also limit, or even avoid, going to public places such as supermarkets, parks, and cultural events [185, 240]. However, immigrant families also demonstrate resilience. Immigrants form new networks [161, 260]; families stay in touch with relatives abroad [80, 307]; and youth adapt quickly through peer interactions and formal education [130, 348]. A prominent theme in this literature is intergenerational dynamics, such as children's roles as interpreters and mediators for their family members [322, 392], or their wrestling with social identities [45, 80, 130, 322].

2.1.2 Immigrants' Technology Use

How immigrants around the world utilize ICTs in their day-to-day lives has been studied extensively, showcasing a community of people who actively engage in technology for a wide range of purposes. Studies have found that immigrants rely heavily on mobile phones

[148] and that ICTs not only help immigrants communicate with those back home, but also aid their integration into new societies [71, 84, 85, 105, 364].

Less research has focused on technology use by undocumented immigrants in the United States, but the existing prior work echoes findings of ICT use among other immigrant populations. Undocumented immigrants use ICTs (primarily mobile phones) to enhance their integration experience (e.g., to find jobs) and to stay in touch with family abroad [38, 39]. Undocumented youth use social media in creative ways to contribute to social movements and to fight for their rights [100]. Gomez and Vannini [162] find differing behavior among undocumented populations attempting to cross the border and those who have already settled in the U.S. And, while Constanza-Chock notes that privacy and security concerns about technology are especially salient for immigrants [100], prior to our study little was known about how technology risks are perceived by undocumented immigrants living long-term in the United States.

2.1.3 Privacy and Security Concerns and Behavior

We live in a world of mass surveillance and unprecedented personal data collection, as evidenced by the Snowden NSA leaks [175], targeted advertising [393], vast quantities of online personal sharing [149], and the digital traces left by everyday activities [329].

Online privacy and disclosure risks on social media, as well as strategies for navigating them, have been studied extensively [129, 193, 374]. People use diverse strategies for managing self-disclosure. Individuals also have to navigate networked privacy and group privacy issues [113, 352], including tensions that arise from "boundary turbulence" [301], i.e., how information about you can be disclosed by others [21, 47, 229, 301]. Lampinen et al. distinguish among three dimensions through which people manage boundary turbulence in social media: preventative and corrective strategies; mental and behavioral strategies; and individual and collaborative strategies [229].

Yet, research on online privacy and privacy behavior suggests that overall, people often do not take protective action [186, 366]. Known as the "privacy paradox" [37, 281], individuals struggle to translate intentions to protect their privacy into action, often sharing potentially compromising information about themselves [177] and regretting it later [380]. Reasons for the privacy paradox include bounded rationality in privacy decision making [4, 5, 302], misconceptions about information flows [18, 217, 235, 315, 335], misconceptions of protective measures [203, 313], and context violations [237, 279]. These issues are exacerbated when people are unaware of the risks involved, or do not fully understand their implications. More generally, Slovic finds that unknown risks are perceived as less dangerous [342]. Furthermore, when technology risks are uncertain, studies have found that trust in companies and platforms serves as a key heuristic in guiding people to override potential concerns [250]. Other studies have focused on marginal risk perceptions, and found that if personal information may otherwise be public, individuals will invest less in protecting it themselves [7].

Companies may exploit decision heuristics to nudge users towards disclosing more information [4, 5, 56]; affordances of social media platforms have been shown to strongly influence users' self-disclosure behaviors [21, 78, 374]. Options for alternate platforms or encrypted communication channels are limited; while security and privacy tools like anonymous browsing [120], decentralized social networking [118, 248], and encrypted communication tools [55, 396] are active research topics, these tools have not been widely adopted. Many studies have uncovered hurdles and usability issues in adopting new security or privacy tools [157, 386, 3].

There is some research on privacy and security behavior of specific vulnerable communities, including teenagers [57], journalists [256], recovering addicts [391], intimate partner abuse survivors [249], parents of LGBT children [49], homeless populations in the U.S. [389], and urban populations in the developing world [83]. These studies reveal nuanced, community-specific concerns and practices. A recent population survey [244] found that many people of low socio-economic status (SES) in the United States are acutely aware of digital harms, feel "very concerned" about digital privacy and security, and display low trust in Internet-service providers. The study also finds that low-SES Hispanic adults are most sensitive to privacy risks, know of few resources to protect themselves, but express high interest in learning how to do so. Studying Muslim-Americans, Sidhu found that despite widespread belief that their online activities were monitored by the U.S. government, few altered their online behavior to address these concerns [337]. Overall, there is no blanket theme that all marginalized communities have in common regarding privacy practices. Privacy risks are varied, diverse, and differ among populations given their individual status and place in society.

Our study contributes to the literature by considering technology issues among an especially vulnerable community, Latinx undocumented immigrants in the United States.

2.2 Background

Threats to undocumented immigrants have intensified recently in the United States [236], where immigration enforcement is in the purview of the Immigration and Customs Enforcement Agency (ICE). ICE already grew substantially under the Obama Administration, with the Trump Administration planning to add 10,000 more ICE officers [273, 357].

ICE has also expanded its technical capabilities. Today, individuals stopped by ICE will typically have their fingerprints scanned, even without arrest [44]. Facial recognition is becoming prevalent: in 2016, Customs and Border Patrol (CBP) solicited proposals for consumer-sized drones equipped for facial recognition and cross-referencing with law enforcement databases [60]. In January 2017, President Trump called to expedite biometric data collection at all ports of entry [359].

Meanwhile, privacy protections for immigrants are being eroded. In 2017, President Trump issued an Executive Order on "Enhancing Public Safety" that removed all protections of the Privacy Act for undocumented residents, thus expanding data sharing between federal agencies [44, 358]. In Vermont, the Department of Motor Vehicles has allegedly been responding to information requests by ICE and other federal agencies by running facial recognition against their state ID database, in violation of its own state law [355]. Concerns over data sharing have been renewed with the recent termination of the Deferred Action for Childhood Arrivals (DACA) program for undocumented immigrants who arrived in the U.S. before the age of 16. DACA granted registrants work permits, drivers' licenses, and a renewable two-year stay of deportation [115]. Post-DACA, how information about DACA registrants will be used is unclear.

How ICE currently uses social media data is not well-documented, but its use seems to be increasing. In September 2017, the Department of Homeland Security published their policy of collecting social media handles of all immigrants, including permanent residents and naturalized citizens [147, 376]. In 2017, ICE officers in Detroit submitted a warrant to Facebook to collect the phone number of an undocumented man. His phone number was then used to locate him by tracking his mobile phone with a cell-site simulator (known as a "Stingray" device) [343].

2.3 Study Design

Between July and September 2017, we conducted 17 interviews with Latinx undocumented immigrants (14 women, 3 men) in an urban area in the U.S. Midwest. These were conducted in-person at a participant's home or in spaces trusted by them (e.g., a church or restaurant). Sixteen interviews were conducted in Spanish by at least one of the native Spanish-speaking co-authors; one was in English. The interviews were audio-recorded and lasted 66 minutes on average, ranging from 52 to 81 minutes.

Before reaching out to potential participants, we spent several months developing relationships with local immigrant rights organizations and community allies to assess how we could best recruit undocumented persons while protecting their privacy. Several allies then distributed advertisements for our study through their networks. Despite going through these trusted channels, recruitment was slow initially. After a first few participants, we were able to reach the other participants via snowball sampling, but even then, we had to follow up repeatedly with potential participants. Especially among men, we faced considerable difficulty in recruitment.

2.3.1 Interview Themes and Protocol

We developed our semi-structured interview protocol through iterative literature review and conversations with allies of the immigrant community. An English version of this protocol can be found in Appendix A.

In order not to be suggestive of sensitive issues, we began all interviews (as well as recruiting) by focusing on technology use in general, avoiding mention of privacy, security or surveillance. We asked about participants' daily lives, community activities, and immigration stories. We then asked them to describe their daily technology use: which devices and platforms do they use, how frequently, and for what activities. We asked participants about frustrations or concerns with the way they use technology. If it did not come up naturally, we then asked whether they had concerns about technology given the broader challenges of the undocumented community. Then, we asked about their privacy and security practices online, eventually probing about security tools, privacy settings, password practices, etc. Finally, we invited them to share any final thoughts or concerns about technology. Demographic data was collected after the interview via a questionnaire.

Participants received $20 for their participation. The study was exempted by our IRB, and documentation requirements regarding payments were waived in order to ensure participant privacy.

2.3.2 Data Security, Coding and Analysis

We followed a strict security protocol in handling participant data. Audio files were encrypted before storing them in our institution's cloud storage, which is certified for sensitive identifiable human subjects data. No unencrypted documents contained identifying information for any participants. Furthermore, we did not discuss sensitive content about our interviews or participants over email.

All interviews were transcribed and translated by bilingual research team members; for the first eight interviews, one Spanish-speaking team member transcribed the Spanish audio recording, then translated the text to English. A second Spanish-speaking co-author spot-reviewed the English translations against the audio recordings. Because quality was high, we translated the remaining nine interviews from Spanish audio recordings directly into English transcripts. Again, a second co-author spot-reviewed the translated English transcripts. All potentially identifying information was redacted in the transcription process.

Qualitative analysis was conducted on the redacted, English transcripts. We used an inductive coding process and thematic analysis. Two of the interviewers identified preliminary themes, which were developed into an initial codebook. Through multiple iterations of independently coding different interviews, each followed by collaboratively revising the codebook, we arrived at a stable codebook with good inter-rater reliability (Scott's Π=.692). One researcher then coded the remaining interviews and recoded the interviews used for codebook development. Using thematic analysis, we explored the 80 codes grouped by overarching categories to identify and analyze prevalent themes.

2.4 Participant Population

Despite our best efforts to seek participants with diversity in age, gender, and occupation, our sample (see Table 1) was dominated by women with children (76%) in their thirties and forties (median 38). They are settled immigrants, the majority from Mexico (88%), who have been in the United States 10–17 years (median 14). Most are part of mixed-status families, with children 1–30 years old. Some have children they brought with them into the United States (29%), but most have U.S.-born children (88%) who are therefore U.S. citizens. The prolonged stay in the U.S., and the establishment of mixed-status families, is typical of the broader undocumented immigrant population in the United States [164].

ID	*Gender*	*Age*	*Origin*
P1	F	40-44	Mexico
P2	F	40-44	Mexico
P3	F	30-34	Mexico
P4	F	30-34	Mexico
P5	M	40-44	Mexico
P6	F	40-44	Mexico
P7	F	40-44	Mexico
P8	F	30-34	Mexico
P9	F	30-34	Mexico
P10	F	40-44	Mexico
P11	M	35-39	Mexico
P12	F	35-39	Costa Rica
P13	F	30-34	Mexico
P14	F	18-20	Mexico
P15	F	50+	El Salvador
P16	M	30-34	Mexico
P17	F	35-39	Mexico

Table 2.1: Participant demographics.

Most participants told us about their journey to the United States. At least two reported arriving by plane and overstaying their travel visas. Most others traversed the U.S.-Mexico border by foot under rough conditions, lacking food and water, and then taking collective vehicles to their final destination. Experiences ranged from taking eight days to up to two months to cross from origin to destination. Most successfully arrived as desired, but a few arrived only after multiple attempts.

2.4.1 Limitations

Gender and place of residence, among other variables, can substantially shape undocumented immigrants' experience of illegality and integration [95, 164, 288]. Our participants were mostly women who all had been in the United States for over 10 years. Undocumented men, individuals who only recently entered the country, as well as undocumented immigrants in other areas, especially close to the border, may exhibit other technology use patterns or risk perceptions. Furthermore, research with "hidden populations" is challenging. Our sample is small and should not be construed as representative. Instead our research was exploratory and provides initial insight into technology's role for undocumented immigrants.

2.5 Findings

Below, we go through our findings in three broad categories: daily offline life as it pertains to immigrant status; general digital technology use; and issues related to privacy and security.

2.5.1 Navigating Risks in Daily Lives Offline

Most of our participants spoke proudly about how well they have integrated into their local communities and their efforts to live as "normally" as possible. Trusted places such as schools, churches and public libraries serve as safe spaces. Nevertheless, there is a fragility to their life, not only due to the ever-present threat of immigration enforcement, but also due to the reliance on good will of employers, local authorities, neighbors and others. Some go to great lengths to protect themselves while others try to avoid constantly thinking about risks. The recent intensification of immigration enforcement has also strengthened many of our participants' commitment to helping other community members protect themselves by sharing relevant information with them.

2.5.1.1 Fears of detention and deportation

The lack of "papers" loomed large for our participants. They expressed a sophisticated understanding of their risks due to lack of legal status. Most mentioned that immigration authorities could show up to detain and deport them at any time, with devastating effects. P12 shared a respective experience: *"They asked [my neighbor] if there were more Hispanics [...] that did not have papers. So, they are not truly looking for anyone in particular.*

They are just searching for someone to take. [...] I was really nervous and got this huge headache, and I thought, 'My son is inside and if they come and take me, what will happen to him?' ICE was there all week, so we had to be careful about going outside."

About half of our participants tried to avoid thinking about their risks constantly, whereas the other half made significant adjustments, as discussed below.

2.5.1.2 Limiting exposure to authorities

Many participants have had direct contact with authorities at various levels (federal, state, local) for issues related to paying taxes, addressing traffic violations, or applying for privileges for their U.S.-born children (e.g., single custody or food stamps). Therefore, they perceive that at some level, authorities already have some of their personal information. Others actively tried to avoid providing information to authorities, even when it meant opting out of potential benefits: *"We've delayed ourselves in getting DACA for our son. It's due now. Lately, when you go and fill out the application, supposedly it's supposed to be confidential, that just your children's information will be on it. But I've heard that they ask for the rent agreement, and we're all on that. There are names, our address, the phones"* (P10).

Driving was frequently mentioned, given that the participants' state no longer issues driver's licenses to undocumented immigrants. Being stopped for traffic violations is mentioned by many as a risky scenario that could lead to greater problems (a finding echoed in prior work [185]). Yet most participants risk driving even with concerns. P11 said *"I drive calmly. I know what can happen, but I try not to think about it."* A few participants have chosen not to drive at all. P10 explained, *"The truth is, I never learned to drive for that reason, because the police would detain me."* While P15 has been driving during her 15 years in the United States, she stated that recent intensification of immigration enforcement led to greater fear when she was on the road.

2.5.1.3 Risks from information disclosures to authorities by others

Two participants mentioned experiences where disclosures by people they knew led to immigration authorities locating them (P14, P16). For example, *"Immigration had gone to my cousin's house and he had a brother who told them I was their cousin in addition to where I worked [...] We try to be careful all the time, but sometimes the problem is not us but other people"* (P16). But for these two participants, the information disclosures did not lead to greater care with their information — there was a feeling that the authorities already knew what they needed to pursue enforcement actions.

2.5.1.4 Intensification of perceived risk

Almost all participants emphasized a mounting sense of risk since the U.S. presidential election in November 2016. In response, participants reported making inconvenient adjustments in their daily activities. P10 recounted how she and her husband no longer leave their child home alone: *"[My daughter] has to get up earlier so [my husband] can take her, because we cannot leave her alone, because we do not know what is going to happen."*

Similarly, P12 said, *"Now we have to be more careful, even in the stores. One sees that they look at you badly, so I'd rather avoid those things. I even avoid talking in Spanish, so I talk to my son in English instead."* She mentioned that many in her community have recently prepared documentation to facilitate child custody in case they were arrested.

Most participants also referenced increased harassment, racism and social stigma in interpersonal interactions over the past year. Many participants felt that strangers are now more open with anti-immigrant sentiments. P12 recounts: *"I was at the pharmacy and my son was talking to me in Spanish, so there was a lady who got mad and told the cashier that they should only allow people who speak English."* Another negative experience was shared by P10: *"My sister-in-law told me a few days ago that she went to a park and saw a woman who asked her, 'Where do you work? That's a nice uniform. Do you clean houses? Where is your permit?' And, very ingenuously, she replied, 'I don't have one.' The lady* *then said Trump was going to take all the Latinos out. It's ugly."*

2.5.1.5 Perceived obligation to share and inform others

Along with the increased sense of insecurity, almost half of our participants mentioned a growing sense of collective identity with other immigrant families over the past year. Technology is increasingly used to share information about the presence of immigration officers, news of raids, or any other immigration enforcement related activities. P1 noted, *"One feels more responsibility in passing on this information."* Such distribution of information was also perceived by participants as an opportunity to regain some autonomy and sense of empowerment.

2.5.2 Undocumented Immigrants' Technology Use

Technology plays an essential role in our participants' lives. All participants used smartphones, with usage dominated by communication with friends, family, and community institutions through apps such as Facebook and WhatsApp.

2.5.2.1 ICT adoption driven by communication and convenience

For many participants, ICTs are indispensable. For example, banking, scheduling doctor's appointments, and receiving information from the schools their children attend, such as grades and absences, are all done online. P11 explained: *"From the school, it comes to my email, so everything goes there directly. When I go to the appointments, it's on my email."* These needs (and how it was often inconvenient to navigate these daily activities without ICTs) were driving factors behind the adoption of some technologies, such as email.

ICTs are also instrumental for communicating with friends and family back home, and in many cases, newer technologies offer significant convenience. P15 stated: *"Before, I needed to buy [international calling] cards at the store. Thunder, raining, or lightning, I had to get these cards. Sometimes I would buy the $25 cards and never use them, but* *when I did, I would have no balance left.... That's why [Facebook] Messenger is a perfect technology, because with it I can talk to my daughters and see my mother."*

Family also played a role in technology adoption. For some participants, family members were the ones advising and encouraging the use of technology. A few participants described how information (such as Facebook passwords) was managed by a family member. Many participants were also motivated by their roles as parents to develop their competency with technology: most expressed a desire to become comfortable with general computer tasks, and expressed concern over their limited ability to assist with homework and prevent their children's exposure to cyberbullying or adult content.

2.5.2.2 Mobile-primary lifestyle

Although many participants own both computers and tablets in addition to mobile phones, all participants use their smartphone as their primary device. A few of our participants also noted that they depended solely on their mobile data for access to the Internet. Convenience and ease-of-use were cited as reasons for this mobile-primary lifestyle. P3 works as a housekeeper: *"In the work I do, everything is now by text, because I no longer answer calls since I'm on the job cleaning with another person. [...] I check how [my daughters] are, to see if they've eaten. With my husband, I use it to look up directions. I even use it to know how to cook turkey."*

2.5.2.3 The central role of Facebook

All but one participant were active Facebook users. Main uses were keeping in touch with friends and family abroad; engaging in their local community; and finding events in their area. WhatsApp was the second most-used tool; primarily used for video calling, voice messaging, and photo sharing with family abroad. Facebook Messenger was used in largely the same way, although mentioned less. A few participants mentioned other tools, such as Instagram, Snapchat, and Twitter, but most comments regarding social media revolved around Facebook, WhatsApp, and Facebook Messenger. All but one participant had Facebook accounts and all but three had WhatsApp accounts. This indicates a heavy reliance on a small and consistent set of tools — notably, all of which belong to a single company: Facebook.

Adoption of tools is motivated by ease of use and people in their networks using them. P12 says *"The only thing I use is Facebook and WhatsApp, because they're the easiest and other apps are too heavy."* When deciding on creating a group for their community, P1 said *"So I did some research and decided on WhatsApp. Everyone has it and it's free, so I downloaded it and added everyone."*

2.5.3 Risk Perceptions and Mitigation in Technology Use

While participants were mostly enthusiastic about the benefits of technology, they reported a range of risks — from common security and privacy concerns unrelated to their legal status to various kinds of unwanted visibility that could lead to more extreme consequences. While participants sought privacy and safe spaces for intimate communication through "network regulation" [374] and careful self-disclosure, channel choice, and a degree of self-censorship on social media, most participants expressed resignation with respect to the risk of immigration-related surveillance.

2.5.3.1 Common privacy and security concerns

Asked about concerns and perceived risks of technology use, most mentioned security-related threats that are not unique to their immigration status — concerns such as identity theft, online financial fraud, unauthorized access to their Facebook accounts, and hackers who might steal their information or impersonate them online. Some also brought up concerns with strangers watching or contacting their children online, and with children harassing and bullying each other through technology. For the most part, technology-related risks regarding their status were not at the top of our participants' minds.

2.5.3.2 Valuing privacy and intimacy

Many participants mentioned a general desire for personal privacy, without explicitly relating it to their immigration status. This desire came up most prominently with respect to social media, especially Facebook. While everyone highlighted the benefits of Facebook, most noted a desire for "intimate interaction," especially with family abroad.

With respect to these concerns, participants saw their privacy and security as largely being in their own hands. Almost all participants reported expending effort on network regulation, curating an intimate network of people to maintain Facebook as a safe space for them. They have restrictive friending practices (*"only friends and family"*): *"I am very selective about social media. I have people who I really know and people I know from far away. I only have family and nearby friends, but besides that, no"* (P3).

Participants also expressed concerns about strangers contacting them: *"There are people we don't know and send invitations as if they were friends. I don't accept just any person if I don't know them. I have a lot of requests but I don't accept them because I don't know them. I only accept those I do know and talk to both here and in Mexico"* (P7).

Two exceptions were participants who mentioned that their network included mostly people who they know but with whom they have looser ties, or even distrust. Given context collapse concerns, they mostly abstained from posting on Facebook to avoid creating windows into their lives.

Overall, most participants displayed trust and confidence towards people included in their curated network, and talked about Facebook as an intimate, safe space.

2.5.3.3 Limiting self-disclosure

While most people regulate their network to keep it intimate, the way participants stated their privacy goals also reveals a deeper sense of concern about unwanted disclosures.

Concerns with photos came up most often. Some participants were happy to post pictures and saw this as an enriching aspect of keeping in touch with family abroad. These participants varied in terms of how they shared photos within Facebook. Half were happy to post intimate content in their profiles, whereas the other half were more cautious. Some of them rarely posted pictures of themselves on their profile pages, and if they did, made sure not to reveal locations or intimate spaces. For example, P12 explained: *"I don't like having everyone see my Facebook. Just people who know me that I interact with. There are photos of my son and friends. I do it overall for my son, because I don't want people knowing where I live, [...] if we're somewhere else, fine. But my house or anything showing my house number, no."*

Specifics about the consequences of disclosures were rarely elaborated on. Only P4 specifically expressed that posting location information could result in physical safety risks: *"The majority of people who use social media, they post their location all the time or where they are, but one doesn't know that someone might come and do something. So, that's my worry, that someone knows where I'm going and tries to harm my family. I'd rather abstain."*

Some only shared photos privately, i.e., one-to-one or in small groups via Facebook Messenger. More broadly, we observed systematic selectivity between spaces/channels offered within Facebook, and the public/private notions about each of these. Participants tended to view profiles as the most public place within Facebook. They viewed Facebook Messenger as the most private channel, where those with reservations about unwanted disclosures are more likely to share intimate content with trusted individuals and groups. WhatsApp was not considered part of Facebook. When asked about preferred communication channels, one participant had a sophisticated notion of WhatsApp's security: *"WhatsApp is more private than Facebook ... because it's encrypted and had other features that other apps don't have. It has more privacy"* (P5).

Some of the perceived risks were tightly bound to participants' home country, but separate from immigration status. Specifically, many of our participants come from regions in Mexico where kidnappings, extortion and physical violence are common. Two participants shared anecdotes about perpetrators using location information from social media in kidnappings back home. P16 worried that details about his lifestyle in the U.S. could be interpreted as affluence and put family members back in Mexico at risk of extortion: *"The problem is that if one posts them, there will be people in Mexico who will see them and think that since one is here, one has enough money and they'd want to do something bad to other family members."*

Many participants raised concerns about participating in digital public spaces. Several people mentioned online harassment, which they credited to a more openly xenophobic atmosphere in the U.S. since Fall 2016. P1 stated: *"There was a link about political topics on [a local news website] and the boy commented on it and there all these racist people came to attack. It reached the point where they quickly found his profile and even where he lived, and they threatened with sending immigration [enforcement] to his family."*

Participants tried to avoid such risks by not engaging in online public discussions. For example, P3 said: *"On social media, I've seen lots of things about people being taken away by ICE. It got me angry seeing reports on the news, because you start to see the comments, and I feel a lot of impotence ... you think and you don't comment back. Mostly, you get upset and you stay that way, because I hear about a lot of people who are afraid for their kids or of being followed and all that."*

However, in digital spaces perceived to be public, some participants opt for more open sharing of their political or social views, although this could sometimes create tensions. For example, P14's view on expressing her political opinion on her Facebook profile differed from her mother's: *"My mom now has been [saying] 'I don't think you should share that, [...] cause when immigration investigates you and they see that, they're not gonna want to give you your papers because you don't like their president.' [I said,] 'Listen, I'll share my thoughts before I get any papers.' "* This situation is indicative of the strains undocumented immigrants in the current socio-political context have to navigate, and the looming sense of resignation that all content can potentially be surveilled and investigated.

Overall, participants primarily managed privacy and security concerns through a limited set of practices: network regulation, varying degrees of self-censorship and deliberate choice of communication channels.

While self-disclosure was the main privacy-related concern mentioned, it was not the only source of stress — just being connected to information networks could be taxing. More active social media users among our participants noted that too much information related to undocumented immigrant issues, such as raids or deportations, weighs heavy on them. While they valued rich information sharing and mentioned technology as a channel for receiving support, they were concerned about effects of information overload on themselves and family members. P2 stated, *"Sometimes it's good to have support from the community, but sometimes it's bad because to be constantly reading this kind of information, it's exhausting. And this is through whatever means of communication, so much as in television, radio — it's all the same. And it's too much."*

2.5.3.4 Concerns about disclosures by others

For undocumented immigrants, privacy takes on a collective character in various ways, with implications for shared responsibility within family units, other undocumented immigrants in their networks, and allies. Others can deliberately or inadvertently disclose information about undocumented individuals or groups via technology in various ways, creating privacy "boundary turbulence" [301] and potentially putting those individuals at risk. Yet, most of our participants did not perceive these as concerns. To the contrary, most only expressed their appreciation for social media groups that were used for immigrant-related information sharing and coordination. Several of these groups have formed in response to increased immigration enforcement risks. Only P2 expressed concern of being associated with such groups. She worried that group members' identifying information could end up in the wrong hands if one of them would be arrested or detained: *"One of the young men they detained was part of the group, so I got worried and thought, if they're* *checking everyone's social media and they find the group, well, they can find me and that's that."*

Concerns about being exposed affected participants' engagement in community activities. Some participants regularly attend events related to undocumented immigrants, such as vigils, informational sessions, or local government public forums debating these issues. A few of these participants were beginning to question the risks of doing so. A few wondered out loud whether they should be concerned with the relative ease with which events in the physical world can leave digital traces, as information, such as photos, could move easily from meetings in physical safe spaces to more public online spaces. These participants raised how important it was that organizers and other attendees were conscientious about protecting undocumented attendees. They sensed a lack of autonomy and control over their information, but they also felt uncertain about the extent to which they were exposed to respective risks. P2 talked about a photo of her taken at an event continuing to circulate and reappear in perpetuity: *"... every time that topic is discussed, my picture shows up [laughs]."* For a few other participants, the risks of exposure related to attending events, was simply seen as too high — although not specifically due to the ways in which technology may exacerbate the risk. They simply avoided immigrant-specific events completely. P3 stated: *"the more you hide, the less you have to fear."*

2.5.3.5 Trust in platform providers

Some participants expressed discomfort with how certain platforms reveal information about them, but in general participants expressed trust in the platforms they use. In response to questions about their conceptions of any adversaries in their technology use, none seemed to consider the service provider as an entity that had access to their data. In fact, the overwhelming attitude was that service providers such as Facebook were looking out for the users' best interests by alerting them if they had a suspicious login attempt or by providing privacy settings that allowed them to control who could see their content. Conversely, although several participants had negative experiences with social media platforms not working as expected, none of the experiences garnered significant frustration or anger directed toward the company. In one example, P14 found that Snapchat was sharing her location with all her friends without her knowledge. When she discovered this, she changed the location permissions on the app and continued to use it, expressing only surprise and confusion as to why Snapchat would suddenly make such information visible. Despite Snapchat's violating her privacy through opaque feature changes, P14 did not express any direct criticism of Snapchat.

Exceptions to the general trust in platforms were expressed by a few participants who noted that WhatsApp shared identifying information with other users in group chats, especially people who are outside their phone contacts. This may include phone number, profile photo, name, and their online status, depending on privacy settings. For instance, P13 felt very uncomfortable that her ex-partner was able to keep track of her, in her words, *"because on WhatsApp, it says when you're online;"* a known privacy issue [67]. Another participant disliked how WhatsApp enabled one of her contacts to add her to a group with others she does not know. She felt that this created uncomfortable encounters and was an invasion of her privacy, so she stopped using WhatsApp entirely. However, opting out like this was the exception among our participants.

Overall, participants who had negative experiences with technology did not hold the companies accountable, but were generally quick to give credit to services that allowed them to manage interpersonal risks, such as unwanted access to information by others and account compromise. Considering that large technology companies have acquiesced to government requests for private information, this view that risks just stem from users, not from the tool (e.g., through warrants or data aggregation across tools), could be problematic.

2.5.3.6 Surveillance concerns and resignation

Throughout, many participants expressed some notions of surveillance, primarily in the form of concerns with "others" having unauthorized visibility of them or their families. This concern is mentioned across technologies, from TVs, social media, messengers, to technology in general. While participants are mindful of which information they share on public Facebook pages or through Facebook Messenger and WhatsApp, there is nevertheless a sense of an omnipresent threat of surveillance by all-encompassing "others" in both public and private areas of the tools they use. For example, P12 says of immigration-related content, *"many people feel afraid of that information showing up on their page and think someone might be watching."*

Five of our participants brought up the specific concern that "the government" has the power to track, observe, and gain access to information about members of the community via technology. For example, P14 stated: *"It's so scary to see that immigration [enforcement] checks everything about you. I mean, you have no privacy. My Facebook could be private, but they could probably see it. They could probably hack into my messages. They could probably do anything. They could probably somehow get to my information on my phone. [After my negative experience with ICE,] I don't think we have privacy. I mean, I basically think they have access to anything they want. Because they did when they came to my house. They knew everything about us. Things that we were private about with others, they knew."*

With regard to membership in immigration-related groups, three participants expressed their uncertainty as they wondered out loud whether it put them at risk of being *"traced"* by ICE. However, this concern did not outweigh the benefit of those groups and participants continued to use them.

For the most part, the risks of surveillance were palpable, yet abstract. Participants could not pinpoint exact risks and instead feared that the government could see anything. Very few reported strategies they had developed to protect against surveillance. P2 described a strategy that her friend insisted they use when talking about political topics: placing their phones in the microwave. P12 avoided using certain words in messages and on social media, she and her friends used code words instead. However, while there is some concern that technology could amplify the risks of detection by authorities, there is a stronger sense of resignation that government authorities already have information about them, regardless of the technology choices they make.

2.5.3.7 Limited precautions

Finally, it is worth stressing that almost none of the participants in this study discussed using the privacy settings and controls available in the respective tools they actively use. While they have some strategies for seeking privacy and security as we discussed, they have a limited sense of risks and trade-offs, and overall are not familiar with the range of choices they could employ to be safer online. We noted little interaction with fine-grained privacy controls, such as post-specific visibility settings or reviewing content visibility. Most participants knew about additional options to further customize privacy settings within Facebook, but did not use them.

2.6 Discussion

Consistent with prior literature [164], our findings show that the undocumented immigrant community is indeed vulnerable in many ways, and our participants felt this vulnerability acutely. While some try to live their lives as “normally” as possible offline, others go to great lengths to mitigate risks. In their ICT use however, few of our participants worried nearly as much and do relatively little to address their vulnerability. While this behavior is consistent with general findings on privacy practices [186, 366], it is in glaring contrast to our population’s level of vulnerability, the potential consequences of disclosure, and the extreme protective measures some of them take offline.

2.6.1 Factors Impeding Effective Privacy Protection

Why does a community with objectively higher risks do so little to protect themselves as they use technology in their daily lives? Madden [244] finds that Hispanic adults in the United States considered to have low socioeconomic status also have low technology literacy. However, our interviews suggest that low levels of digital literacy are not a sufficient explanation for our participants. There are at least four additional factors: (1) technology provides tremendous benefits to this community; (2) there is significant uncertainty about ICT-related risks specifically associated with their status; (3) they have high overall trust in the major social media platforms; and (4) a general belief that authorities are omniscient leads to a sense that any protective measures would be ineffective.

2.6.1.1 Benefits outweigh uncertain risks

Past research suggests that risk perception is based on two factors: how known the risk is, and the 'dread' factor of the risk [342]. If the risk is unknown, perceptions of its danger will decrease. Our participants did not see a direct line between technology-related actions and potential immigration-related consequences. There are few examples of technology leading to immigration enforcement, and there are no tangible clues in the digital environment that help users understand risks. This uncertainty likely contributes to a perception of low risk, which is in stark contrast to offline interactions, where risks are more tangible and better known. Most participants strove for a balance between unconstrained use of technology and complete abstention. For some, the benefits — communication, information and self-expression — outweighed uncertain risks. A small minority chose to abstain from engaging in social media and group communication.

2.6.1.2 Trust overrides critical risk assessment

Our participants place a relatively high degree of trust in their tools, likely bolstered by observations of peers actively using those tools and a sense of control over their data [59].

In addition, participants display trust toward the companies and platforms that mediate their online interactions. No one shared perceptions of harm or danger in relation to companies, even though these companies amass data for commercial interests and have to provide law enforcement access in certain circumstances. Scholz and Lubell [330] found that trust may serve as a heuristic that leads to the circumvention of effortful cognitive processing of potential risks. The trust our participants placed in service providers may lead them to bypass critical consideration of their role in disclosing sensitive information.

2.6.1.3 Resilience with resignation

Our participants took few privacy-enhancing actions in part because they felt that authorities have plenty of information about them. In this, they echo previous findings that if people already think their information is available elsewhere, they may be more reluctant to try to take precautions [7].

2.6.1.4 Similar behavior, amplified consequences

Most of our participants' security and privacy concerns were similar to those of the broader population, including concerns related to identity theft, monitoring children's online behavior, and unwanted contact by strangers. Studies among college students have found a broad range of strategies in managing self-disclosure and interpersonal disclosures [229, 374]. Our participants' privacy regulation strategies are similar, but different in two ways: First, they are limited to a few kinds of individually-focused, preventative behaviors primarily aimed to enable "intimate interaction" [374]. Second, the boundary turbulences they experience have amplified consequences.

Furthermore, while our participants have developed clear ideas about what physical spaces are relatively private or public, safe or less safe, these notions are eroding through the encroachment of technology. Social norms about how to protect others' privacy and security in shared communities are still underdeveloped. Everyone has a camera in their pocket, and the ability to instantly post photos with geolocation could jeopardize the safety of those depicted. Boundaries blur between online and offline privacy and security, which also affects boundaries they have expended much effort curating online.

Finally, the burden of self-censorship on a person's well-being can be oppressive [373, 374]. Extra stress could have negative implications for integration, further isolating undocumented persons and their families from the broader community.

2.6.2 Implications and Recommendations

Based on our findings, we have identified insights and recommendations for digital security education, community organization, and technology design, which may benefit not just undocumented immigrants but vulnerable communities in general.

2.6.2.1 Develop community-appropriate educational resources

Most of our participants felt their digital literacy was not as developed as they would like. We see an opportunity for educational resources about digital security developed for immigrant communities that incorporate their identities as individuals, parents, and undocumented immigrants. Indeed, almost all our participants were eager to improve their technology literacy and better protect themselves.

However, they do not seem to seek out available online resources, which means that compiling resources online — even if optimized for mobile — is insufficient. Instead, knowledge could be brought into the community, preferably in the community's primary language; participants expressed strong interest in in-person trainings and workshops on technology use, privacy and security. Such efforts should be carefully discussed, coordinated and led by trusted community allies and support organizations. Done well, ICT educational efforts could contribute to the overall well-being and integration of undocumented and mix-status immigrant communities.

2.6.2.2 Take precaution with organizational communication practices

Allies should be aware of the risks of potentially revealing information about members in vulnerable communities. Organizations that hold information about their patrons and community members may inadvertently put undocumented immigrants at risk. Those that have a strong interest in protecting undocumented immigrants in their community, such as schools, churches, activist groups, and libraries, should evaluate their technology practices. For instance, special care should be taken when collecting or storing phone numbers given that their exposure could facilitate locating individuals.

2.6.2.3 Building new tools is not a priority

While designing new technology is a frequent impulse to help vulnerable communities, it is rarely successful [362]. From our interviews, it seems unlikely that our participants or their communities would adopt new tools or apps of their own volition. The fact that this community is largely not using fine-grained privacy settings further suggests that current privacy settings and tools might not be properly meeting users' needs. Furthermore, apps aimed at this community would stand out as observation targets for immigration enforcement. Instead, the focus should be on improving existing tools and on making privacy and security features more visible and usable.

2.6.2.4 Support on-demand information hiding

We find that this mobile-primary community carries and stores much of their digital information on their smartphones. If lost, searched or confiscated, smartphones may put the owner and others at risk. While many smartphones are already fully encrypted, the proliferation of usable authentication mechanisms, such as fingerprint or face recognition, may weaken practical security, as a person could be compelled to unlock a phone with biometric markers if detained [323]. More research should focus on means to enable information hiding on demand and plausible deniability on smartphones. An example in that direction is a feature in Apple's iOS 11: quickly pressing the home button five times temporarily deactivates fingerprint authentication and forces passcode entry [383].

2.6.2.5 Make information flows and audiences more transparent

The uncertainty about online risk of exposure contributes to concern and stress for most of our participants. The transparency of who has access to information and what entities participate in information flows requires further research attention. Prior research has shown that privacy nudges can increase awareness of a social media post's audience [379]. Research on increasing awareness and accurate understanding of information flows would benefit not only undocumented immigrants but also Internet users in general.

2.6.2.6 Limit exposure of identifying information

Service providers could reduce privacy concerns in group settings by limiting what group members can learn about each other. For instance, while messaging apps may rely on phone numbers as identifiers, phone numbers may not have to be visible to everyone in a shared group, making it more difficult to extract group members' contact information. Service providers and researchers should study and consider how desired affordances of social media platforms could be maintained while providing the opportunity for vulnerable communities to protect their identity on the platform.

2.6.2.7 Virtual sanctuary for undocumented immigrants

Companies, such as Facebook, should recognize that they are serving a variety of vulnerable communities, many of whom believe the platforms provide a safe space. They may want to embrace the role of guardian and protector of those communities. Platforms could strive to provide virtual sanctuary. This would mean re-examining what information their services collect, store, share, and expose to other users, in order to reduce opportunities to harm vulnerable communities with the data they have been entrusted with. These companies may also want to consider adopting stances akin to sanctuary cities in the United States. We hope large companies like Facebook, as transnational companies, would strive to protect all of their users, regardless of socio-political or physical borders.

2.7 Conclusion

For undocumented immigrants living in the United States, typical struggles of immigration and integration are exacerbated by a fear of discovery and deportation. How undocumented immigrants perceive and manage status-related risks in technology use has not been well understood previously. Through our interviews with 17 Latinx undocumented immigrants, we provide insights into this community's technology use, risk perceptions and protective strategies. We find that many struggle to translate the awareness and risk mitigation strategies they employ in the physical world to technology use and the online environment. Due to uncertain risks of various kinds, including surveillance and a sense that the government knows a lot about them already, many do not fully consider how their behavior online may affect risks of discovery. For others, technology use is associated with tensions among convenience, intimate engagement, self-disclosure, self-censorship and community participation. Furthermore, we find latent yet uncertain concerns about what others in their network might inadvertently reveal about them. These tensions and boundary turbulences create stress that may affect their well-being and that their families.

Our findings demonstrate an opportunity for reconsidering the design of transparency and privacy mechanisms, as well as the design and provision of educational resources. Community organizations, such as schools or churches, as well as service providers, such as Facebook, also have an important role to play in mitigating, or potentially exacerbating, risks for undocumented immigrants and vulnerable communities more broadly through their information collection and use policies.

CHAPTER III

Safety is More than Security: A Case Study of Digital Sex Work[1]

Since the rise of the Internet, there has been a massive increase in the number of sex workers working partly or exclusively through online [106]. Sex work is prohibited or heavily regulated in most countries, resulting in many sex workers needing to manage digital and physical risks carefully while carrying out their work. Even in countries where sex work is legal, the profession is heavily stigmatized [326], and working legally may not be an option for all workers [305, 351]. Furthermore, sex work can be a risky business: in person, sex workers may face aggressive or violent clients, and police or immigration action [208, 305]; online, sex workers may face doxxing, harassment, or having their content stolen or misused [209]. Much like other end-users — but unlike previously studied at-risk occupations such as journalists [257] — sex workers rarely receive specialized digital security and privacy training or customized security tools.

Further, sex workers make up a sizable portion of the population: an estimated 42 million people are engaged in sex work worldwide [289, 242], spanning all genders, ethnicities, and socioeconomic backgrounds [268, 205, 327]. A growing body of sociological and HCI

[1] This chapter is based on: Allison McDonald, Catherine Barwulor, Michelle L. Mazurek, Florian Schaub, Elissa M. Redmiles. 2021. "It's stressful having all these phones": Investigating Sex Workers' Safety Goals, Risks, and Practices Online. In the 30th USENIX Security Symposium (USENIX Security). [251]
This project was supported by the Max Planck Institute of Software Systems. Allison McDonald was supported by a Facebook Fellowship.

research has looked at how the Internet has impacted the working conditions of sex workers, including how they find and interact with clients [40, 73], conduct their businesses [327, 326], and even the forms of sex work they do (for example, supplementing in-person sex work with camming: live performance of sex acts on camera) [106, 210, 334]. Yet, while many recent studies on digitally-mediated sex work touch upon safety management [326, 327], none, to our knowledge, center the digital safety experiences and technical needs of this high-risk population.

Our research goal is to elucidate how sex workers manage their digital privacy and security. By understanding how a population that knowingly operates in risky physical, legal, and social contexts makes decisions around digital privacy and security, where the consequences of unwanted exposure can be significant, we hope to better understand (1) how technology can better address the specific safety needs of this particular population, (2) how awareness of serious risk influences digital security and privacy behavior, and (3) whether existing safety strategies and tools leave some needs unmet or force unwanted trade-offs. A better understanding of how this population manages digital safety can also inform our approach to improving digital security for end-users more broadly.

Through 29 semi-structured interviews with sex workers in Germany and Switzerland and a survey of 65 sex workers in Germany, Switzerland, and the UK (all countries in which sex work is legal but regulated), we explore sex workers' self-defined safety goals, the risks they identify to those goals in terms of both adversaries they frequently defend against as well as the digital tools that make protecting themselves difficult, and the concrete strategies and tools they use to protect themselves against those risks.

Safety for our participants encompasses multiple axes, including physical safety, financial security, having and enforcing clear boundaries, respect, privacy, legality, and access to a community of sex workers. Each of these axes of safety is dependent on others; a threat to one axis may increase the risks from another. For example, a sex worker failing to keep their legal name private may increase chances of physical threats like stalking or blackmail.

Our participants describe complex safety strategies, such as the use of multiple devices, self-censorship online, and the creation of support communities, e.g., to warn each other about dangerous clients. Yet, despite being aware of risks, and despite the serious consequences of failing to protect themselves, few participants engage with traditional tools specifically designed for privacy and security such as privacy settings, Tor, encrypted chat platforms, and password managers. Sex workers view these tools as lacking sufficient efficacy to address their risks or merit the effort of use. Instead, our work suggests the need for a more comprehensive re-imagining of what it means to be safe online, beyond individual tools and settings, including scaling the home-grown protections that high-risk users such as sex workers develop for themselves out of necessity, such as multiple identities, and protections that address both online and offline axes.

3.1 Related Work

Digitally-mediated sex work. Sex work is defined as the exchange of sexual services for money, encompassing a broad range of services such as escorting (i.e., full-service sex work), erotic massage, porn acting, camming (performing live sex acts on video), phone sex, professional domination (performing the dominant role in a BDSM relationship), and erotic dancing. Sex work is increasingly digitally-mediated, offering both new opportunities and challenges [208].

Prior work has examined the impact of the Internet on sex work through an economic lens. In 2011, Cunningham and Kendall found that the rise in digital sex work was due to overall increases in the commercial sex market and not from the migration of street-based sex workers to digital spaces [106]. Sanders et al. also found that, in 2016, 35% of escorts based in the U.K. were doing some form of digital sex work in addition to outdoor sex work [326]. Workers engaging in digitally-mediated sex work also had higher earnings than outdoor (street) workers [106]. Prior work suggests these economic gains are related to the Internet's utility as a tool for advertising to clients, allowing sex workers a greater amount of control over their ads and the clients they accept [327, 73, 40]. The Internet has also enabled new forms of sex work that are entirely digital, like camming [210]. Furthermore, the increased prevalence of the Internet has created new spaces for digital activism and community among sex workers [140].

The Internet can also reduce sex workers' risks. Strohmayer et al. describe the ways that sex-worker support services use digital technologies to better provide services [347], and in subsequent work examined in particular the *Bad Client and Aggressor List* used by sex workers in Canada to share warnings about potentially dangerous clients with one another [346]. Additional work shows that digital mediation of sex work reduces rates of law enforcement interactions, in turn lowering the risk of harassment or arrest [73, 106].

Nonetheless, sex workers still experience risks online and offline, and the Internet is increasingly intertwined with their safety management strategies. Several studies have discussed how sex workers manage risk via the Internet. Moorman and Harrison examine Backpage ads to learn how sex workers in the U.S. manage risk through carefully crafted ad language, and find that risk management differs across race and gender, with Black women and transgender sex workers exhibiting the most risk management [268]. Sanders et al. find in their survey of U.K.-based sex workers that most (80%) had been recent victims of crime, and enumerate ways they manage risk through strategies like using pseudonyms on digital platforms, screening for bad clients in forums, and relying on social media to have safety check-ins with friends or partners [327]. In this work, we build on existing knowledge of sex work risk management to hone in on the relationship between safety goals and risk management strategies, focusing on where digital safety strategies succeed and fail.

Digital privacy & security. There is an extensive body of research on tools and strategies for digital privacy and security. Multiple studies have examined the usability of various security tools and privacy enhancing technologies like encrypted chat (e.g., [3, 2]), Tor (e.g., [156, 387]), passwords and password managers (e.g., [54, 203]), and two-factor authentication (e.g., [128, 96]). General themes from these studies suggest that managing complex systems (as privacy and security tools often are) is difficult for many users, and the trade-offs users make based on perceived costs and perceived risks may lead to low adoption of even well-designed tools [43, 189, 319]. In this work, we examine whether users who perceive their digital risks more concretely, and who have arguably more severe risks, utilize more or different tools and protective behaviors.

Other work has focused specifically on how marginalized or otherwise high-risk populations manage privacy and security. Lerner et al. found that among transgender people, the Internet provided significant benefits in terms of activism and promoting representation of trans people, while creating new risks like blackmail and doxxing [234]. Guberek et al. studied privacy and security behaviors of undocumented immigrants, finding that participants took few concrete steps to protect their digital privacy and security [179], while Simko et al. examined U.S. refugees' digital privacy and security, finding that cultural differences impacted knowledge of digital risks, as well as the usability of security mechanisms like account recovery questions [339]. In prior work examining a high-risk occupation that depends on the Internet, McGregor et al. studied journalists' digital protective strategies and found that participants stopped using or were unable to use some secure tools because they were disruptive to or incompatible with their journalistic workflow, and that using secure tools with sources was challenging because both parties needed to use the tool for it to be effective [257]. Building on this prior work, we examine a high-risk population whose members frequently have multiple, intersecting high-risk identities, including gender identity [205] and immigration status [351]. Like journalists, sex workers often use the Internet for work, but without the specialized training or tools journalists often have.

Additional prior work has examined how technology is used in relationships with intimate partner violence (IPV) to create harm [187, 152, 249], while yet other work has examined end-users' security and privacy considerations during online dating [159, 94]. Our work focuses on digital security and privacy within commercial, regulated sexual contexts rather than non-commercial relationship contexts, though some risks may overlap.

3.2 Methods

We seek to understand (1) sex workers' safety goals; (2) the privacy and security challenges sex workers face in achieving those goals; and (3) the strategies workers use to mitigate those risks and achieve their safety goals. To answer our research questions, we conducted, in late 2018 and early 2019, interviews (n=29) and surveys (n=65) with sex workers in European countries in which sex work is legal.

Ethical considerations. As our participants are members of a high-risk population, we not only consulted with an ethics review board but also hired a sex worker to review our study materials for ethics and appropriateness. Further, we took care to protect participant privacy and ensure, as much as possible, that our work does not risk identifying participants. Specifically, we (1) collect no personally identifiable information, including collecting no demographic data, and (2) use end-to-end encrypted tools in all study communications. As we did not collect participants' demographics, we use gender-neutral pronouns for all participants throughout the work.

3.2.1 Participant Recruitment

Our recruitment strategy was designed to capture a broad range of sex workers and their experiences, within legal, regulated contexts. We recruited interview participants by distributing recruitment flyers, both in English and German, at brothels in multiple cities, at multiple points of time, in Germany and Switzerland. We further contacted brothels and sex work organizations via email and phone calls. Organizations that were willing distributed our advertising materials to their constituents. Lastly, participants were recruited through snowball sampling, where participants recommended other sex workers. Participants were incentivized with an additional 10 Euro/CHF for referrals. Hard-to-reach populations like sex workers are often studied via such participant-driven sampling [207, 17, 262]. However, such sampling methods can limit generalizability. We used our multi-method recruitment approach to maximize generalizability — fewer than 10% of our participants came from snowball sampling.

Participants signed up for the study via an online form. They were given the option of creating an anonymous ProtonMail account for scheduling and for compensation, or providing an email address of their choosing. Overall, the recruitment process for this study took over four months; our experience collecting data is described in more detail in [317].

Participant descriptives. While we did not collect demographic information to ensure the anonymity and establish trust with our participants, many participants mentioned aspects of their identity during conversation. We can therefore describe at a high level the plurality of identities that our participants held, which shows that our sample, much like the sex worker population in Eupope [351], is diverse across many identities. Our sample contained sex workers who identify as both men and women, and not all of our participants identify as cisgender. Our sample contained participants that are immigrants from Eastern Europe, North America, and Africa, and participants who had varying levels of work authorization. Not all participants were white. Finally, the sex workers we spoke to varied in age and work experience; some had just begun working in the last year, while others had been working for multiple decades.

3.2.2 Interview Data Collection

Interview protocol. In our interviews, we sought to understand the safety goals, risks, and protective behaviors of our participants. Participants were first asked background questions to understand the type of sex work the participant performed and how they typically used the Internet in their work and personal life. Next, we probed their experiences of safety, asking questions such as “What is safety to you as a sex worker? How do you define safety?”

We then probed their perceived risks (e.g., whether they have had a negative experience online, what types of attacks and attackers they aim to protect themselves against). We then explored participants' strategies for maintaining their online safety (e.g., "Would you say you do anything in particular to maintain your safety online?"), including probing specific behaviors such as use of security and privacy settings. Lastly, we asked participants questions about additional sex-work-related topics, outside the scope of this project.

Interview procedure. Participants chose to be interviewed either via chat, voice, or video. As such, there are quotes that may contain text-speak or emojis. Based on each participant's language preference, interviews were conducted in English or German by members of the research team fluent in that language. Interviews lasted on average 60 minutes, ranging from approximately 30 minutes to 2 hours. For participant safety, all interviews were conducted using private paid "rooms" on Appear.in,[2] an end-to-end encrypted communication service. Participants were paid the equivalent of $75USD (75CHF or 60 Euros) in the form of an Amazon gift card or money transfer.[3] Following each interview session, audio recordings of the interviews, if applicable, were transcribed in the native language. German transcripts (both chat and audio) were then translated into English for analysis; bilingual members of the research team consulted the original German transcripts during analysis to ensure that tone, turns of phrase, and cultural contexts were captured and included in quotes and coding.

3.2.3 Survey Data Collection

After conducting interviews, we developed a survey instrument to gain a larger sample size and quantification of the same topics and emergent themes explored in our interviews. Specifically, we used an open-response question to probe respondents' definitions of safety: "How do you define safety as a sex worker? What does it mean for you to be safe?"

[2] Appear.in recently changed its name to Whereby.com.

[3] Sex workers in Germany and Switzerland earn between 50 and 600 Euros per hour; thus we aimed to compensate them appropriately for their time participating in our study.

Four closed-response questions asked about respondents' use of different digital tools (e.g., encrypted messaging applications, Tor); their use of safety strategies mentioned by interview participants (e.g., "I only communicate with clients on certain devices, SIM cards, or apps"); and how legalization of sex work and immigration status affected respondents' feelings of safety. The interview protocol can be found in Appendix B.[4] Survey participants were recruited from sex workers who contacted us to participate in the interview after interviews had concluded (early 2019), and were compensated 10EUR for roughly a 10-minute survey. As in our interview study, respondents could take the survey in either German or English.

3.2.4 Analysis

Interviews were analyzed using an open-coding process. Three co-authors randomly selected four interview transcripts to identify emerging themes and create a thematic framework for the interview data. After creating a codebook, two of the co-authors independently coded 10 interviews to reach clearer insights into the interview data. All interview transcripts were then double-coded, codings were reviewed by the researchers after every two to three interviews, and any disagreements were reconciled. Because the interviewers reviewed every independently-coded transcript together, we do not present inter-rater reliability [265, 255].

Responses to the open-response survey question about safety definitions were similarly analyzed using the same codebook. The results of our closed-response survey questions are reported descriptively. As this work is exploratory in nature, we had no hypotheses and thus make no statistical comparisons.

3.2.5 Limitations

Our results may be limited in their generalizability and by participants' willingness to share sensitive experiences. While we did our best to use many recruitment methods,

[4] Additionally, the interview protocol, survey questions, and codebook can be found at `https://osf.io/9mj7k/`.

conduct our study in multiple languages and at different sites, use non-judgmental language, and offer participants a high degree of privacy to encourage sharing, we cannot be sure that we exhaustively captured all possible experiences and strategies of sex workers in countries where sex work is legal. However, our results provide a set of concrete insights into the experiences and safety strategies of a high-risk population, not previously studied in the security literature.

3.3 Results

Based on the responses from both interview and survey participants,[5] we describe the privacy and security goals of our participants, the threats they see to those goals, and the strategies they use to protect themselves.

3.3.1 Definitions of Safety

We identify seven common safety goals. Most participants mentioned *physical safety*, and many talked about *financial security*, *clear boundaries*, and *privacy*. For some *respect*, *legality*, and *access to community* were important safety aspects. The ways that our participants define safety are intimately connected with their digital security needs and guide their protective strategies. By considering our participants' holistic safety goals [318], we can better understand their decision-making processes and unmet safety and security needs. While we describe each safety goal separately, these goals are interconnected and were often discussed together by participants. For example, both financial security and privacy may be necessary to minimize the risk of physical harm.

Physical safety. Most participants' definitions of safety included physical safety, which often encompassed being protected from physical assault or threat of assault by aggressive clients. As one survey participant stated, safety means *"being able to work without fear*

[5] We use participant IDs to refer to interview (P) and survey (S) participants.

of abuse or aggression" (S36). That said, not all participants feared for their physical safety. Although we cannot report safety fears by gender due to participant protections, one participant's response suggested that their race and gender impacted their sense of safety: *"Since I am a very privileged white cis male I don't think about safety so much."* (S12) This difference in safety concerns across race and gender is consistent with other studies [268].

Many participants discussed physical safety as being related to having the necessary resources — including supplies, a safe physical space in which to work, and access to healthcare and the ability to enforce safe sex practices such as the use of condoms — to safely do their work. P11 describes:

> "Safety for me means: I can do my job in an environment that doesn't endanger me and provides me with the necessary stuff to protect me. I need gloves and condoms, for example. I also like to not be raped and killed on the job, so I prefer working in a studio with colleagues present." (P11)

Some participants described safety as when their protective strategies — including digital strategies — were in place (we discuss protective strategies in more detail in Section 3.3.3). For example, one participant shared:

> "I'm safe when people know where I am. . . I like when the clients send me photos before of them because when I don't know the face of the guy I am very scared." (P10)

Financial security. For many participants, financial security is a primary component of safety. Participants mentioned that financial security depends on sex workers being compensated fairly and having access to health insurance and other government and social safety nets. Financial security also ties closely into physical safety. For example, several participants mentioned that when they are financially secure, they are able to turn away clients who make them feel unsafe. For example, S31 explains:

> "I don't use drugs, don't gamble, have no debts, no financially needy relatives etc so I feel zero pressure to accept bookings. . . if I had to accept jobs against my better judgement eg someone who's obviously drunk or aggressive... or demanding services I don't offer, I would be unsafe." (S31)

Clear boundaries. Many participants' definitions of safety involved ideas of boundaries, psychological well-being, and, as S9 put it, *"to have control."* Participants reported feeling safe when their physical and sexual boundaries were respected, but also when their personal time was respected, as well as when digital boundaries they established between their work and personal lives were honored. P8 describes:

> "Safety is knowing. . . that my boundaries won't get crossed, like pushed to have unprotected sex. That I'll get paid for what I asked and that the hours will be clear and done." (P8)

Respect. Many participants connected their safety and well-being to being respected by clients and society at large. S10 stated that safety means *"not feeling that society thinks it's normal for me to get hurt."* P20 expands on this idea, saying that safety is intertwined with being protected from discrimination and stigma:

> "The absence of fear of suffering personal or financial disadvantages due to one's activity. . . where the rule of law prevails over personal reservations. Working as a [sex worker] should be recognized as a normal job." (P20)

Privacy. Respect and privacy are often linked. P6 says:

> "Privacy is directly tied in with safety from harassment these days. Safety is about working safe in a society that treats me with respect and respects my privacy as well." (P6)

For others, feeling safe is directly connected to their ability to control the privacy of their personal information from clients and/or from their social networks.

> "For me, privacy is when clients don't know my name or address and can only contact me when I allow it. . . . An unannounced visit from a friend would be something nice. An unannounced visit from a client would be a catastrophe." (P14)

Many participants worried about being "outed," or publicly identified as a sex worker against their wishes. The potential consequences of being outed range from embarrassment to blackmail and threats of physical violence. P10 shared:

> "I have a friend who [was blackmailed]. And if she didn't pay [the blackmailer], [they] would tell all the . . . neighborhood . . . My friend was born in a Muslim family, so it's more difficult. . . . If her family knows it, and if neighborhood knows it, she said to me that it would be the end of social life for her family." (P10)

This demonstrates how closely related privacy and physical safety are: if privacy goals are not met, it may lead directly to physical danger.

Legality. For some participants, safety stems from working legally and having access to support services:

> "I want to be recognized as a legit business. I want to tax my income and also deduct my expenses. I want to qualify for social security. I also want a safe way to advertise and find clients. I want to be protected by law, if a client misbehaves." (P6)

S22 describes how working in environments where clients feared law enforcement — because the location where they were pursuing services was not in compliance with legal regulation — makes their job less safe:

> “[I want] to work as little as possible in ‘gray / dark’ environments, such that customers [don’t] have the feeling of needing to hide - [then] it is easier for me to vet them ahead of time.” (S22)

For some participants, like P6, safety meant being able to call the police if they had a negative experience or were in danger. However, among our participants the ability to call the police safely might depend on whether they were officially registered as a sex worker, which was often, in turn, related to their immigration and work authorization status. Thus, some participants instead described safety as minimizing contact with the police as much as possible. S2 explains:

> “One of my sex worker friends is an undocumented migrant. . . She has no right to access healthcare. She is very distrustful of police and the authorities. She guards her privacy and anonymity more than other sex workers I know.” (S2)

Access to community. Having access to a support community of other sex workers can also be an important component of safety. These support communities may be online or offline, as suggested by other work on sex workers [327, 140]. These online spaces can provide emotional or logistical support in the case of a negative experience, or just a place to feel validated and less isolated. S52 identifies that to feel safe, it is important for them to *“ensure I get things off my chest. . . with other sex workers in-house or online when I can.”*

While these communities can provide safety education and resources, participants may face significant barriers to achieving and maintaining them. Policies regulating the use of online platforms for sex-work-related topics, even if not used for sex work itself, threaten the existence of these communities.

3.3.2 Perceptions of Risk

We next discuss the sources of risk identified by our participants. Unsurprisingly, clients pose a significant threat. Risks from clients often manifest on multiple safety axes. For example, clients may violate a sex worker's boundaries by finding their personal Facebook. If the sex worker's legal name is exposed, this can create risks of stalking and blackmail, which in turn increases risks to their physical security.

However, risk also stems from the legal and technical landscape in which sex work is conducted. Laws that regulate sex work (or business more generally) create opportunities for unwanted information exposure. Similarly, digital platforms create information exposure risks through the ways they moderate content and (dis)allow sexually-explicit uses, which may threaten the financial security and physical safety of participants. Finally, even the non-sexual policies of digital platforms — like "real name" requirements and people recommendation algorithms — create privacy risks for sex workers.

Risks from clients. Clients were often the most direct threat to workers' *physical safety*. Several participants shared stories of physical assault, while many others discussed experiences with harassment and stalking:

> "If you decide to close the [work] relation[ship] [some clients] become obsessive. A couple of times. . . I have been blackmailed, threaten they'd expose my activities online to my peers and family. Others have just showed up on my place of work looking for me. . . It's very unsettling, but with the right precautions I've learnt to avoid it. I'd much rather lose money than meet someone with potential to cause problems." (P17)

Efforts to avoid dangerous clients may threaten a participant's *financial security*. Furthermore, the threat of stalking and blackmail from clients often led participants to not only focus on physical safety, but also discuss the importance of *privacy*. In particular, keeping their real name and location private from clients was important for staying safe both online and offline. As P11 stated, *"I don't want clients to show up at my university or worse, at my flat. Some clients can get attached."* P24 had similar concerns, and shared a story illustrating the intersection between *privacy* and *physical safety*:

> "My lovely partner, who is also a photographer, has photographed me a couple times. I wasn't very smart and published my photos with his tag on a relatively public forum. . . Then, a client of mine who was very fond of me — which I also wasn't totally aware of — did some research and figured out who my boyfriend is. He found our places of business and then of course knew what we do in our free time, what our names are. . . Since then, I pay extremely close attention which tag is on the pictures." (P24)

While some negative experiences with clients may pose physical safety risks, other participants described clients threatening their *boundaries* by draining workers' time and resources: "time-wasters" just looking to chat or ask for photos without intending to book a session.

Legal risks. The extent to which sex work is legalized, and how it is regulated, influences how safe many sex workers feel while working. Our interview participants worked primarily in Germany and Switzerland, where sex work is legal, but several had also worked abroad in countries with different legal frameworks. Their experiences both in Germany and Switzerland, as well as abroad, highlight that the different ways *legality* is defined impacts their safety. Several participants noted that when countries follow the Nordic model, in which selling sex is not illegal but buying sexual services is [305], they feel less safe. Our survey supported this: two-thirds of respondents reported that whether they were legally permitted to work as a sex worker affected how safe they felt. One participant explained that this was because clients are more afraid and less willing to share their real information with sex workers when the client is buying illegal services; sex workers rely on this information to vet new clients, or to check that an unknown client does not have a bad reputation among other sex workers [40, 346]. P10 described related challenges from working in France:

> "If guys want to see escorts they [must] pay like 1,000 Euros if they are [caught]. So that makes the job more difficult because you have to stay in this in secret.

> . . . If you have a problem you can't [call] the police." (P10)

Even when working in a country where sex work is legal, a worker's immigration status may prevent them from legally registering as a sex worker. Of those we surveyed, 20% reported that they felt "insecure" or "very insecure" because of their immigration status. In particular, our participants described how the inability to work legally due to immigration status or the country's legal framework results in a lack of access to law enforcement, trustworthy clients, healthcare, and other safety nets, leading to risks to *physical safety*, *respect*, and *financial security*.

Even among those who are eligible to work legally, discomfort with the way legalized sex work is regulated can create safety issues. For example, as of 2017, German sex workers are required to register in order to work [69]. Some participants worried about how the government might use such data about them. Two participants shared that the registration requirements reminded them of the Nazi era:

> "The registration and the new law, that concerns me. . . . I don't want to give them all my data. . . I feel like I'm in the 30's. Of course I have concerns about that. . . [will] the moment ever come where there are like, online raids and people try to track our profiles?" (P12)

P26 had similar thoughts, and said, *"maybe the [registration] data isn't being mishandled today, but in the future it could be."* This highlights the tension between *legality* and *privacy*; in order to be compliant, sex workers in Germany must sacrifice personal information that they may feel puts them at risk.

According to P16, the registration requirement also creates divisions between sex workers and makes it more difficult for sex workers to organize together, as their goals and needs are different. This creates barriers to building *community*, which in turn creates a barrier to staying safe:

> “There is absolutely no worker solidarity between the German workers and the non-German workers. They’re happy for all of us [non-German workers] to basically die in the gutter, and it’s very frustrating. I blame the way that the laws are set up in Germany, because it puts sex workers into two camps, those who are legal and compliant with German law, and those who. . . still need to work, but they can’t get licenses.” (P16)

Several of our participants also expressed anger at the ways FOSTA-SESTA impacted their work even in Europe. FOSTA-SESTA is a 2018 law passed by the United States Congress, which was purportedly designed to remove protection from liability for websites that facilitate sex trafficking. The effect was that many sites that sex workers had used to advertise, screen, and build community, including Backpage.com, were taken down or categorically excluded sex work from their platform [16, 77]:

> “Backpage was really great and SESTA/FOSTA really sucks. . . especially here in Germany where my job is totally legal and I pay taxes. Pretty frustrated. [It used to be] about 30% of income and I still didn’t recover from it. Backpage was very easy to use for clients.” (P13)

P2 worried that FOSTA-SESTA and similar laws would soon block them from all platforms they use to do sex work:

> “When I see stuff like FOSTA, it’s also a question of time and when Europe will become similar. And then there’ll probably be nothing left for us except to manage everything by hand.” (P2)

Non-sex-work-specific laws also impact the safety of sex workers. For example, Germany has an imprint requirement for websites (“Impressumspflicht”), requiring websites to list the website operator’s legal name, address, and contact information [117]. Many participants mentioned that this requirement threatens their *privacy* and potentially their *physical safety* because they must either list their real contact information on a site on which they otherwise use a pseudonym, or risk being in violation of the law.

Risks from digital sex-work platforms. Even digital sex-work platforms pose safety risks to sex workers. Several participants reported having their intellectual property — photos of them or composed advertisements they had created — stolen and republished on other sex-work advertising websites that they had never used before. The business strategy of these websites is to steal workers' ads with legitimate photos and contact information in order to draw in customers, hoping that when the sex worker whose content has been stolen begins receiving calls from clients who found them on the new site, they choose to begin using the website in earnest. Sometimes, these new websites use workers' photos to advertise services the sex worker does not actually offer, creating risks to their *physical safety* if a client contacts them expecting those services. The participants to whom this happened described having their content stolen as an upsetting violation of their *boundaries* and *privacy*. Potential recourse, which might involve commissioning a lawyer to send a take-down notice, was described as "too laborious" (P14) or unlikely to be successful:

> "I haven't been able to get mine down. . . . I know a lot of people have [tried very hard], and they don't take them down. And that's the thing with being criminalized, it's like where do we even turn? No one cares about people stealing your stuff." (P18)

Risks from other digital platforms. Sex workers also experience harm on non-sex-work digital platforms due to platform rules and community standards. American-based digital payment platforms, like Paypal, are especially challenging for sex workers. Paypal offers a popular and simple way to transfer money, but is not a reliable tool for sex workers. Many of our participants reported having accounts frozen or deleted, sometimes blocking access to their funds. This is likely done under Paypal's "Acceptable Use Policy," which prohibits "transactions involving. . . certain sexually oriented materials or services" [298].

The lack of reliable, common payment platforms, and the risk that popular payment platforms like Paypal will freeze or disable their accounts, sometimes left our participants with difficult choices for processing payments and made *financial security* more difficult. While many still use cash primarily, cash posed challenges for large payments and for digital sex work. We discuss participants' strategies for working around these limitations in Section 3.3.3.

Even when workers do not use digital platforms for sex work, they may experience harms due to their identity as a sex worker. Many participants talked about how they could not use American social media platforms to discuss, let alone advertise, their legal sex work services because these platforms had rules against sexually-explicit content. One participant shared their experience of being banned from a social media platform without warning or notice:

> "I had I don't know how many followers on Instagram and at some point. . . it was just deleted. . . that definitely hurt my business . . . since a lot of clients say, yeah, where can I find pictures of you or something and then I would just send a link to my Instagram account and that was convenient." (P4)

As P20 put it, *"Google is now a market driver and one has to submit to their 'norms.'. . . Or Facebook."* In many cases, there is no recourse to being banned [40, 33].

Similarly, two participants talked about being banned from AirBnB, despite never using the platform for sex work — as far as they can tell, their identity as a sex worker alone was enough to get them permanently banned from the platform:[6]

> "AirBnB bans workers just for being [sex workers]. They have not shown their face, don't use same email or phone. . . and they don't [do sex] work from [an] AirBnB and they got banned." (P13)

[6] AirBnB filed patents for technology that allows them to identify sex workers and those that are mentally ill in 2018 [119], but reports surfaced regarding AirBnB discriminating against sex workers as early as 2016 [297]

While digital platforms such as PayPal, Facebook, and AirBnB are based in the U.S., they operate at a global scale. The imposition of American-driven community standards on sex workers working legally has significant repercussions for nearly every aspects of workers' safety we identified above: physical, financial, privacy, and the ability to set boundaries and create and maintain community.

Digitally-mediated interpersonal risks. Digital platforms can also enable or facilitate risks to sex workers from other platform users. Several participants described challenges with platforms that require them to share their legal name. P3 explained how this made Paypal dangerous by exposing their legal name to clients when they pay:

> "Being able to use Paypal would be awesome. . . [it doesn't work because] we're all criminals. And I work under an alias. Paypal doesn't allow that. Paypal and also Amazon are U.S.-led companies. You'll be kicked out if you do sex work" (P3)

These "real name" policies have long been documented as dangerous or damaging, for example for trans people who have not had a legal name change [112, 183]. For our participants, many of whom use an alias when they work for safety purposes, such policies risk exposing their legal name to clients, and thus threaten participants' *boundaries*, their *privacy*, and potentially their *physical safety* by increasing the risk of stalking or blackmail.

Instances of digitally-mediated context collapse, in which a platform forces the intersection of previously distinct audiences [246], had similar consequences on our participants' goals. Multiple participants discussed having clients contact them through a social media or dating site that they did not use for sex work, or friends and family finding their sex work accounts. Sometimes this is a direct result of platform design rather than deliberate snooping. For example, Facebook's People You May Know (PYMK) algorithm is known [377, 190] to cause this issue:

> "I wanted a second account with Facebook [for clients to interact with me]. I had a different email address. . . I didn't want my friends to see it at all, but they were suggested to me [by Facebook] immediately. . . [so] I just deleted it right away." (P29)

Regardless of the mechanism through which a sex worker is found, the experience is violating and threatens workers' established *boundaries*:

> "Somebody found my [private] Tinder profile. . . . I did simply explain to him that I found that a bit stalking-like what he was doing. And that I didn't appreciate such personal contact. He carried it so far to search and find my private Facebook profile, then I blocked him. I don't want to have personal contact with my clients on my Facebook profile.. . . That also destroys my image as dominatrix." (P21)

While some described strategies for avoiding these privacy violating experiences (see Section 3.3.3), others shared this sentiment with P23: *"there are things that are just unavoidable."*

3.3.3 Safety Strategies

Many participants took steps to meet their safety goals and avoid potential threats to those goals. Rather than being technically complex, participants mainly relied on manual protective strategies, such as vetting clients, self-censorship, and keeping two separate devices. While technology made some of these strategies more effective, few participants relied on security tools to be safe online. Often this was due to security tools and features being a burden, disrupting other safety strategies, or being difficult for clients to use, leading to a lack of adoption or abandonment.

Covering. A common strategy our participants used to protect their *physical safety* is to "cover," or tell a friend or colleague the details of an appointment beforehand, so that they can contact the police or another emergency contact if the person does not check in at a pre-planned time. This strategy was used by 68% of our survey respondents. P2 described their strategy, and how the Internet helps them feel safer:

> “Someone almost always knows where I am. I’ll put out some updates in regular intervals, call someone or do a video chat or something. . . . My safety system without the Internet would. . . not completely fall apart, but. . . it wouldn’t be as comfortable. And also not as comprehensive.” (P2)

However, the effectiveness of covering depends on having a reliable contact to provide cover, and on being diligent about checking in while at the appointment. P5 shared a story about forgetting to check in with their contact:

> “In the heat of the moment I forgot to check the time and then someone knocked on the door and there were two men and the hotel manager at the door and it was then, of course, super embarrassing.” (P5)

Several participants described wishing that there were better mechanisms for doing this without needing to depend on other people, which can be cumbersome and unreliable. P27 envisioned an app or other digitally-mediated platform that could possibly fill this role:

> “Especially for women. . . [who] don’t speak the language. . . . they would enter where they are and for how long and they could push a button to say that they’re there. And then after the time runs out again, that they’re out again. Of course, with a generated password each time. When that doesn’t happen. . . the person that you entered as an emergency contact gets contacted by the app. If you don’t have anyone, then it’s the administrator that alerts the necessary authorities.” (P27)

P27 also suggested that if this type of covering tool existed, it would also work as a deterrent for aggressive clients, and that *“probably it would be enough, if johns knew that there was something like that.”*

Vetting clients. Some interview participants talked about vetting clients prior to meeting them in person, and 51% of survey respondents said they gather information about clients before meeting them.

Vetting can take two forms. In the first form, sex workers use their networks to check information from the client (for example, name or phone number) with friends or in private online forums, in order to see whether a client has a bad reputation among other sex workers or had been reported for being violent. These forums might contain others' reports of negative experiences, complete or partly obscured phone numbers, or physical descriptions of bad clients, similar to the *Bad Client and Aggressor List* described by Strohmayer et al. [346].

One participant mentioned the National Ugly Mugs, which maintains a large, centralized digital services for reporting and searching clients in the U.K. [269], but expressed frustration that the service only covered the U.K. In Germany and Switzerland, our participants did not mention such a centralized service, and several complained that the lack of such a service made vetting clients difficult.

Participants reported that vetting networks and platforms — centralized or otherwise — were not without issues, such as incompleteness or inconsistent formatting of data that makes search difficult.

Vetting also depends on the ability of the worker to get accurate information about the client before meeting them. Some participants reported that clients' willingness to share information depended on buying sex being legal, as fear of being caught would lead them to hide their information. P2 described facing several such challenges when vetting clients through shared online databases:

> "It's always dependent on what information I'm provided with. . . If I don't get anything, then I can't search for anything. . . . The problem with that is that there's really no databank. There isn't anything standardized. [It] would just be better, if it would run centrally. And that there would be standards. A main

> problem with those forums is that the phone numbers are never consistently entered." (P2)

In the second form of vetting, the screening process is less about checking for previous bad behavior, and instead intended to *"separate the wheat from the chaff"* (P20). This type of vetting was also reported by Moorman et al. [268]. This was often a strategy developed over time and through trial-and-error, and might be beneficial in both protecting their time and finding respectful clients. P6 described how this process also helps filter out clients who might push other boundaries as well:

> "I optimized my contact method over the years to find a system that provides me with a way to weed out idiots. Making it quite high maintenance to contact me — [by making them contact me] in a very particular way — makes it easier to make sure that those who follow my protocol really want to book me. . . . In my experience, if I have high obstacles and people are willing to take them, I can expect them to also follow my [other] rules later." (P6)

With both forms of vetting, participants said they used blocking features liberally when clients or potential clients were rude or pushy with their boundaries, e.g., within WhatsApp, on advertising platforms, or for phone calls and SMS.

Managing digital identities. *Privacy* is a critical safety goal for many sex workers, and also a goal that helps to facilitate other safety goals including maintaining *boundaries* and protecting *physical safety*, for example from stalking. Sex workers' efforts around digital privacy and security largely focused on ensuring that the digital identities used for work could not be connected back to their legal identity or contact information and ensuring separation between different digital identities.

To protect their identities, many participants described using an alias while doing sex work, and 77% of our survey respondents reported using a fake name or otherwise concealing information about themselves from clients. One worker even developed a service that would allow them, and other workers, to avoid using their real name and address while satisfying German website imprint requirements: *"I helped to develop and offer a service where sex workers can use the official union address as their address for their websites to secure their privacy"* (P6). This is one example of how having access to a community, in this case a workers' union, helps promote safety.

Some sex workers are "out," or public about being a sex worker in their personal lives. However, being out is not a binary; multiple participants who considered themselves "out" still had family members who did not know, or social contexts in which they did not want to be known as a sex worker. For example, P3 said they don't worry about sex work advertising sites collecting personal information, but at the same time they are careful about keeping some personal information off of other platforms:

> "I try to keep my real name out from Facebook. My dad is on FB and he doesn't know what I do. My address, where my boyfriend lives. He works for the church. That is not allowed to come out. . . My [website] imprint is through a third party." (P3)

P14 also explained how being out does not necessarily mean that clients know their personal information: *"It's actually strange, because I'm 'out' privately, but none of my clients know my real name or my address."*

As an alternative to providing false information, or not providing information at all, some workers provide details that have an element of truth but still protect their privacy. For example, P19 described how sharing information that's close to accurate but still vague helps their business by making clients feel special or trusted:

> "It's also a marketing strategy. A lot of guests are also interested in the person behind the dominatrix, so I give them something to 'chew on.' " (P19)

Finally, many participants protect their privacy by maintaining multiple digital profiles (one or more for work and one for personal use) and attempting to keep those profiles separate through the use of separate accounts or even devices (66% of survey respondents):

> "I had only one mobile for a long time, but then [I got another one]. . . . You give your number to people, and at one point they come up with the clever idea to google the number, so they can see immediately what you do for a living. . . . And I started to work a lot with WhatsApp statuses. And then there is the problem that if you want to post a WhatsApp status for work, you want maybe a picture that is a little bit more suggestive. And it is not so good if your private circle of friends sees that, because not everybody knows what you are doing." (P21)

While keeping separate devices was common, it is also burdensome, and not all participants chose to do it over the long term:

> "For a long time I had another phone with a different number and different WhatsApp but then I noticed that it was just too much work for me, separating them. And then I was also really slow to get back to [clients]. Then that went under and I just found it easier to just have one number." (P12)

P18 describes the cost of keeping separate identities:

> "I mean obviously I wish that sex work wasn't considered shameful and I could post to my heart's delight. It's also time consuming and it's annoying, stressful. It's like even though my family knows, I know it would be embarrassing to them if I came out as a sex worker, for them to have to explain that to their friends. That's bullshit, but it's true. It's stressful having all these phones and personas and things I have to remember. I'm like, 'Shit, did I miss that when I put this up?' All the time." (P18)

Beyond finding it difficult or not worth their time, participants also mentioned that financial incentives might motivate them to make exceptions to otherwise keeping their digital accounts or devices separate. For example, P1 described a client who found their personal social media account, an action for which they would normally block a client. However, for one particular client, they said: *"He added me [on social media] after he spent [a lot of money] in a 3 days row :D can't really be mad at him :DDD"*

Self-censorship. While our participants sometimes had considered reasons for relaxing or changing their rules around keeping separate identities, the consequences of digital identities merging or linking back to participants' personal lives or information can be significant. In order to avoid this, some of our participants went beyond maintaining separate profiles, or using false names, to minimizing the amount of information they have online at all.

Out of fear that clients will find their personal Facebook profile or be recommended to them through PYMK, P13 decided to keep their information on the profile extremely limited: *"I don't have photos. I don't have my city or school or uni."*

Keeping photos off of work accounts is more difficult, as the photos are used to advertise. For these accounts, our participants protected their identities by carefully curating photos so that their face or identifying features like tattoos were not visible (46% of survey respondents).

Participants also mentioned removing content from their phones before crossing borders, for fear of being searched and deported. P18 went as far as to completely shut down their online accounts when traveling:

> "I delete my whole work phone, everything incriminating on my computer. I take down my website, I take down all my apps. . . . If they feel suspicious for some reason as I'm crossing and they search all my stuff I don't want that to lead to getting deported." (P18)

This practice was mentioned even by those working legally:

> "I am legally allowed to work in most countries where I work. [However,] I am scared of getting banned from certain countries just for being a sex worker so I remove all my info, account and website and wipe my phone before travelling." (S11)

However, as with keeping separate devices, some participants stopped using such measures because they were too cumbersome or felt ineffective. P16 describes the decision to no longer hide their face in photos:

> "I used to always blur out my face, which I don't do anymore. That was a conscious decision that I knew would make me less safe. . . . I was tired of doing a lot of photoshopping, and partly because I felt a little bit safer in my work at the time, which I don't know if I do anymore, but. . . you can't take back. And clients connect very strongly with faces, so it's a good marketing move." (P16)

Managing security & privacy settings. Few interview participants depended on privacy and security settings within their devices or online accounts to stay safe online. This was reflected in the survey, where only 35% of respondents reported changing security and privacy settings to be more private or secure.

Of interview participants who did discuss modifying settings, the two most commonly mentioned settings were visibility settings on Facebook and location settings on mobile devices. These settings, reasonably, correspond to some of the more tangible physical risks that participants face — being outed unintentionally, and being located or stalked. P18 explained how they changed their privacy settings to avoid being found on Facebook:

> "I used to get a lot of 'Do you know this person' about clients, even though we never interacted on Facebook. I've never interacted with these clients on Facebook and I don't remember their real name or anything, but they would pop up. . . . It's not so good. I had to make everything private." (P18)

A few participants expressed doubt that security and privacy settings would be effective. As P8 put it, *"If we are online, there isn't a lot of hope for privacy."* P21 explained that they do not trust privacy settings, and instead will opt for physical or hardware solutions such as removing a phone from a room, or using multiple devices, to make sure their mobile phone does not collect information they do not want it to:

> "I don't really trust the whole system in this respect. I think it doesn't matter if you put [settings] on or off. In case of doubt the phone will listen in, go along, take notes. Sometimes, when I have to talk about something, I mind that there isn't a phone in the room." (P21)

That people do not or cannot rely on in-platform settings to regulate their boundaries has also been observed in the general population [388].

Security-focused tools. Similarly, few participants mentioned using tools specifically built for security and privacy. In our survey, we asked whether they used several security tools: encrypted messaging applications like WhatsApp or Signal (32% reported using), a VPN (14%), encrypted email (9%), Tor (9%), Password Managers (8%), or cryptocurrency (5%). Interview participants reported two main barriers to using such tools: feeling that the tools were too challenging to use — either for themselves or their clients — or feeling that the tools were not sufficiently effective given the effort necessary to use them. P21 describes a friend setting up encrypted email for them, which P21 no longer uses:

> "I have an acquaintance who [will] only write encrypted emails, but that's very effortful. . . . [They] had to download an extra program for me. There you always had a key and then you had to mess with it forever until you could read that email, this was way too stupid for me." (P21)

Security tools can also get in the way of participants' work or other safety goals. P16 explained that they previously used a VPN to obscure their location, but stopped because it created new privacy risks and interfered with their business:

> “Many VPNs will sell your data. Also, many of the advertising platforms either are partly location-based or won’t let you use their services if you’re not coming from the country that they’re based in. One of the U.K. [sex work advertising] platforms. . . you have to have a local phone number and be accessing that website from an IP within that country.” (P16)

Particularly of note, although many of our interview participants described having problems with payment processors and two even lamented the lack of anonymous payment platforms, none described using Bitcoin or another cryptocurrency. P3 said, *“I’m not enough of a techie for that. . . [and] nobody’s ever suggested it.”* Instead, most sex workers relied on cash. How well this works, of course, depends on their type of sex work (e.g., cam performers cannot collect cash from viewers).

Further, even if a sex worker felt they were sufficiently skilled to use a security tool, and felt that the tool was sufficiently beneficial, their clients may lack the digital skill or interest to use such tools. One survey respondent commented on our list of protective strategies:

> “I would gladly do all of the above, but that really only works when the customers participate: Threema / Signal / Telegram, PGP-encryption, cryptocurrency...” (S49)

As S49 points out, all parties must use it before a new tool like a messaging app or payment system can be useful. This barrier of needing others to also comply with a security protocol was similarly identified by journalists looking to communicate securely with sources [257].

Resignation and regret. Finally, some of our participants expressed resignation or apathy about safety. Some participants felt there was little they could do to be *“100% safe at this job”* (S15). This led some participants to disregard safety practices because they felt that the behaviors are not effective or that harm is inevitable — a common response to corporate surveillance [124]. P25 said:

> "When I think about it, it's like how safe are you, really? How protected are you, really, when Google can find you anywhere, Facebook can find you anywhere? I think the aspect or the perception of safety is a little like, you can be found if someone really wants to find you. It's not so difficult anymore, especially with online presence and everything else. It really depends what you're trying to achieve." (P25)

P13 described how despite the serious risks for them, keeping accounts separate in the course of using them day-to-day felt impossible:

> "I login to Kaufmich [a sex-work advertising site] in browser on my personal phone and my Apple account for work phone is registered to my passport name. . . . I hate myself for it sometimes. . . . This stuff could get me killed or deported. . . . I am not prepared." (P13)

Several other participants similarly described feeling regret about taking insufficient precautions. Some expressed that they had originally made choices they felt were unsafe when creating an account, but now felt stuck with those choices; as P16 put it, *"You can't erase what you've done on the Internet."* This sense that it's impossible to correct past mistakes may keep some workers from engaging in more careful privacy management in the future.

3.4 Discussion

Sex workers experience salient risks both offline and online. Our findings show that our participants have nuanced and multidimensional conceptions of safety and a clear understanding of both digital and offline risks. While physical security was a critical part of safety, safety also included financial security, respect, privacy, legality, clear online and offline boundaries, and access to a community that could help support safety practices. Participants' safety strategies must thus simultaneously support multiple safety goals.

We further identify the primary sources of risk and safety strategies of this high-risk population, who often need to use the Internet to do their work but also face significant consequences if their strategies fail. While our participants have well-developed sex-work-specific protective strategies like covering and vetting clients, many online strategies relied on logical or physical mechanisms — e.g., having two mobile phones, carefully keeping photos with their faces off the Internet, and self-censoring in both work and personal online spaces — rather than using, e.g., platform integrated privacy settings. Few participants used dedicated security tools, and those who did were likely to abandon them, either because they felt the tools were more work than they were worth, or because they disrupted competing work and safety goals.

3.4.1 Building for Sex Work

Ultimately, many of the risks our participants face are not solvable by improved privacy and security tools. Instead, explicit discrimination by social media and payment platforms, poorly designed and explicitly anti-sex-work laws, as well as stigma from the general population, contribute to a dangerous work environment for sex workers. Solutions to the largest problems depend on collective action leading to changing perceptions of sex work, policy changes, and legal changes, rather than the strategic deployment of technical solutions.

With this in mind, we identify two primary ways in which technical tools can enhance sex worker safety. First, existing tools could be modified to accommodate the use cases and threat models experienced by sex workers. Second, new safety tools that specifically address currently unmet sex worker needs can be created.

Refining existing tools. Existing tools are especially well positioned to address *surveillance* risks (e.g., at the border while traveling internationally, by police or governments, or by cross-platform tracking and data aggregation). However, upon examining why these tools are not widely used, we found that many violate other critical safety goals.

In particular, encrypted messaging tools like Signal and WhatsApp could help sex workers keep message content private from both government and corporate surveillance.[7] However, because both applications only allow a single profile per phone number, safely using Signal or WhatsApp with both work and personal contacts might further depend on having a second SIM card or phone, lest the wrong audience see the wrong name or profile photo. In this case, an application with otherwise desirable security properties (e.g., end-to-end encryption and blocking features) becomes harder to use safely for someone with a need to communicate simultaneously with disparate audiences. This design is not necessary for the functioning of the tool — either app could likely enable some limited number of profiles per account without necessarily sacrificing other security properties like end-to-end encryption.

Similarly, VPNs and Tor may offer some protection from surveillance, but their value significantly decreases when they disrupt the user's ability to access the forums or platforms they depend on to stay safe, as one of our participants experienced when they were unable to access geolocation-based vetting platforms. Platforms that manage access through IP location risk denying access to legitimate users who need a VPN [252].

Protecting workers during interactions with clients is another space in which existing digital security and privacy tools have the potential for impact. The safety goals here are usually to keep personal information from clients, keep work information from family and friends, and to be able to draw boundaries and cut off contact with clients when they become aggressive. In these cases, having access to fine-grained privacy and visibility settings may help some workers (those who know about them and trust them), but our participants found that even this careful management fails due to invisible data aggregation, resulting in being outed through people recommendation algorithms or having personal accounts blacklisted

[7] WhatsApp no longer keeps messages to businesses private, and continues to degrade user protection from corporate surveillance [121]; we include it here because at the moment it remains the most popular encrypted messaging application.

because of their work account's activity. Over time, failure seemed inevitable. These issues suggest that many social media platforms continue to fail users who have multiple identities to manage, and that reviewing and changing a platform's data-use policies can be as critical as creating intuitive front-end settings.

Finally, one major risk to workers' financial security, a dimension of safety, was lack of access to digital payment platforms. Cryptocurrencies offer anonymous digital payments and thus might seem like an obvious solution. However, virtually none of our participants used tools like Bitcoin. Cryptocurrencies introduce additional difficulties: getting clients to use such services, even if workers are comfortable using them, and the need to convert between currencies in an already-difficult banking situation. Thus, the vast majority of our participants turned to the analog solution, cash, despite having its own set of problems.

In this case, cryptocurrencies serve as a useful example of how questions of access and usability are not the first that researchers and technologists should ask when building or improving security tools for high-risk users. Rather than considering how we can make cryptocurrencies easier to use for sex workers and clients, we should consider whether they are addressing the fundamental need in the first place. For many, they do not. Our participants need simple anonymous payments, but Bitcoin and similar tools are massively complex systems that do not provide anonymous digital cash. Instead, they provide an entirely independent currency that fluctuates wildly, requires currency brokers and new accounts, and puts users at risk of a massive network of targeted attacks seeking to steal account credentials.

Opportunities for new tools. As articulated by our participants, there may also be opportunities to build bespoke safety tools that better support sex workers specifically.

For example, P27 describes their ideal covering app, which could help sex workers stay safe without a dependable community. Additionally, while there are no technical mechanisms currently available to prevent photos and ads from being copied and republished, there may be opportunity for automating copyright take-down requests for major sites that steal and republish content.

Usable safety tools for sex workers have the potential to support the safety and independence of a sizable population. However, as can be seen from other security tools, if not well-grounded in the experiences of sex workers and their particular legal context, tools can be at best useless and at worst harmful. Design and operation of new tools and platforms should include, and ideally be led by, sex workers. Several sex work and technology collectives like Assembly Four [35] and Hacking//Hustling [181] offer models for this type of collaboration.

3.4.2 Designing Across Diverse Populations

In many instances, sex workers provide another data point showing that many common digital mechanisms can amplify risk and complicate protective strategies. In other instances, however, their needs may diverge from other high-risk populations. This tension should be considered when looking to design for a given community and in building general-purpose tools.

For example, being able to use a pseudonym or keep profiles unlinked from their legal identity is critical for the safety of many of our participants, as it sometimes also is for trans people [112], drag queens [263], and intimate partner abuse survivors [249], among others. Our findings underscore why identity management online is an important security and privacy issue, and may suggest that allowing users to have fully pseudonymous profiles — that is, even unlinked from emails and phone numbers that could be used elsewhere — may reduce the risk of digital boundary violations that lead to stalking and harassment [253]. Even in cases where users do the work to keep profiles separate, unwanted and unexpected intersections of work and personal identities online through friend recommendation algorithms or through being identified by use of a shared, single phone number or email across personal and work platforms can cause significant problems.

At the same time, sex workers themselves depend on having the real — or at least persistent — contact information for clients to vet them and keep track of their behavior and preferences. If fully pseudonymous or anonymous profiles were in place on many of the platforms sex workers use, they could find themselves facing new safety challenges, as existing vetting systems may fail. Furthermore, anonymity on social networking sites can enable further abuse and harassment, which is frequently levied against women, minorities, and other marginalized groups [360].

3.4.3 Broadening the Scope of Security

Beyond designing specific technical tools, our results underscore the multidimensional nature of digital safety. Our participants had well-defined ideas of what they needed in order to stay safe. However, many of the elements that were central to their safety goals, like financial security, boundary regulation, respect, and even physical safety, are often not central to the design and study of security and privacy tools and experiences. Our work adds support to a growing body of evidence [318, 187, 152, 249, 231, 198, 151, 360] that online safety involves axes beyond — but intertwined with — digital security and privacy. Thus, we encourage future research and development to holistically consider the multidimensional aspects that comprise users' safety experiences. Security researchers and developers must revisit their assumptions about risk and benefit to better align with the needs articulated by their users [216].

3.5 Conclusion

Through interviews and surveys with sex workers, we examine sex workers' safety goals, their perception of risks to those goals, and the behaviors they employ to mitigate these risks. Our participants expressed that their safety was defined across multiple interrelated axes, and they perceived risks to their safety from clients, platforms, and legal entities. Our results suggest that sex workers are not only aware of the risks presented by digitally-mediated sex work but are also employing multiple ways to protect privacy and security while online. However, they often rely on manual strategies, such as using multiple devices, as current tools do not balance effort and efficacy well enough to address their safety needs and goals. Our findings demonstrate the importance of studying high-risk populations, in order to develop better security tools to protect both those populations and users in general.

CHAPTER IV

Perils of a Universal Identifier: Phone Numbers as a Case Study for Risky Design[1]

In both Chapter II and Chapter III, we observed how digital identifiers create risk for high-risk populations. For example, through online group chats relying on phone numbers as account identifiers, undocumented immigrants face the risk of entire community networks being exposed should one person have their device confiscated. In this chapter, we use these insights to conduct a deeper investigation of the role of phone numbers in particular in creating these privacy risks when used by companies to identify and authenticate users.

"It took only an hour for my cellphone number to expose my life," wrote Brian X. Chen in *The New York Times* in August 2019 [81]. As a consumer technology writer, Chen had asked a security researcher to expose as much information about him as possible using only his phone number. Right away, the researcher obtained his home address, the full names of his immediate family members, phone numbers he had previously owned, his property tax records, and his (lack of) criminal history. Although the researcher did not use this information for any nefarious purposes, he noted that if he had wanted to, he had a good

[1] This chapter is based on: Allison McDonald, Carlo Sugatan, Tamy Guberek, and Florian Schaub. 2021. The Annoying, the Disturbing, and the Weird: Challenges with Phone Numbers as Identifiers and Phone Number Recycling. In Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI '21). [253]
This project was supported by the University of Michigan School of Information. Allison McDonald was supported by a Facebook Fellowship.

chance of getting into Chen's personal accounts, scamming his family out of money, or even taking over his phone number.

Although in this case no real harm was done, Chen's article highlights just how much information is available about us online and often connected to us by one key piece of information — our phone number. While a phone number used to serve as an intentionally public piece of information listed in community phone books for the convenience of one's friends and neighbors, these numbers now serve a far broader purpose. A phone number can reveal a significant amount about a person. In the hands of a company that relies on advertising, a user can have their online identity tracked, sold, and potentially exposed through data breaches or bad privacy practices [370]. In the hands of an individual, a phone number could reveal a person's physical location, their private online accounts, and provide direct, intimate access to them [102].

At the same time, it is becoming increasingly difficult to participate online without giving out one's phone number. Phone numbers are commonly required to create accounts for online services and mobile apps, and have become a default way for services and companies to identify their users [275]. Searching or uploading phone numbers from an address book is a common way to find acquaintances on social media platforms and in messaging applications, requiring users to share phone numbers to connect on platforms that do not otherwise need them.

Furthermore, phone numbers may be far less persistent than they ought to be for the many purposes they now serve. Unlike other numeric identifiers, such as a social security number, it is very likely that someone else will be assigned a person's phone number when they 'stop' using it. In 2018, the Federal Communications Commission (FCC) reported that approximately 35 million phone numbers are recycled in that way each year in the United States [139]. This reuse carries a huge potential risk: the accumulation of multi-factor authentication (MFA) codes, bank alerts, personal messages from friends, doctor's appointment reminders, and job offers [150, 123] can sum up to a potentially vast amount of information about a person, potentially giving the new owner access to accounts associated with the phone number and sensitive information about the previous owner.

In this work, we broadly characterize the issues faced by individuals related to using phone numbers, and in particular highlight the consequences of phone number recycling and phone numbers being used as identifiers by online services and mobile applications. Companies rely on phone numbers as convenient identifiers for their users, assuming that a phone number uniquely identifies a single person, persistently over time, and that users are comfortable and able to share their phone number with the company and with other users through an app or service. As we show, these assumptions lead to a host of potential privacy, security, and access problems for individuals. Exacerbating these issue and creating further problems are the ways that phone numbers change hands through number recycling, creating inconvenience for new owners of a number and exposing personal information about the previous owner.

We conducted a qualitative study with 195 participants, using an online survey with open-response prompts to elicit participants' negative experiences with phone numbers and the consequences they faced due to how their phone numbers were used. Our participants frequently reported issues caused by phone number recycling, unwanted exposure, and temporary or permanent loss of access to their phone number. The personal consequences of reported phone number issues included harassment, account access problems, and privacy concerns. Based on these findings, we discuss how the assumptions companies make about the utility of phone numbers as identifiers can be faulty and can lead to these issues, and explore design and public policy directions to mitigate risks with phone numbers.

4.1 Background & Related Work

We discuss work related to the identification and authentication of users and general issues related to phone use and phone numbers.

4.1.1 User Identification and Authentication

Digital identity and user authentication have been long-standing security and privacy challenges, as well as issues in economic, social and political contexts [178, 53, 324]. Traditionally, identity systems have been physical, e.g., a passport or identity card. The emergence of digital technology has introduced novel forms of identity and authentication including biometrics, passwords, and phone numbers [178, 395]. With the increased shift to digital interactions, companies and services have needed to establish ways that customers can identify and authenticate themselves online.

Most commonly, online accounts are connected to a person's username (sometimes an email or phone number, sometimes an alias) in conjunction with a password. The username serves to identify the user and the password proves ownership of the person accessing it. Passwords, however, are notoriously challenging for users to use effectively [146] and are susceptible to account hijacking and data breaches [333, 398, 230, 160]. While password creation policies and password meters have improved the strengths of passwords, users still practice unsafe password behaviors [369, 224], such as password composition being influenced by the online service's context [384]. Moreover, passwords tend to be shorter and weaker when created on mobile devices [259].

As an inexpensive alternative to passwords, many companies and services have begun using control over a phone number as a way to prove ownership of an account, especially in the mobile ecosystem [277, 170]. This allows users to log in without needing to remember a password; an application, for example, might send a one-time code to the phone via SMS, which is then entered into the application to prove control of the phone number. However, as has been shown with email [312], an authentication message that is sent to the wrong person due to mistyped or recycled phone numbers can create account security risks.

Access to a particular phone number may also be used for account security. Multi-factor authentication (MFA) is a means to mitigate some risks associated with passwords without completely replacing them. MFA often takes the form of a password and a mobile phone, where the possession of a mobile phone is proven through SMS time-based one-time passwords [321, 227] or an app-based authentication code.

Recent work has shown that SMS-based MFA can be relatively effective in protecting online accounts, but performs worse than other second factors against account compromise. Doerfler et al. found that SMS-based login challenges prevented 96% of phishing attacks and 76% of targeted attacks [122]. Due to hijacking risks with SMS-based MFA [336] and the availability of more effective second factors, the use of SMS as a second factor has been discouraged by the National Institute of Standards and Technology (NIST) in favor of hardware and software token generators [172].

In addition to a rise in the use of phone numbers for MFA and account authentication, the prevalence of mobile technology has shifted how users interact with and store their data online [75]. This means that phones and phone numbers provide a high value target. For example, SIM-swapping attacks, in which a person convinces a mobile phone provider to switch someone else's number to a SIM card they control [28], have increased in recent years and can have significant financial consequences when used to access banking and digital currency accounts [306].

4.1.2 Common Uses of Phone Numbers

Online services and mobile applications increasingly request or require users to provide their phone number for a variety of reasons. Privacy implications of targeted advertising with phone numbers have been studied, for example, showing that phone numbers shared for MFA are also sometimes used for targeted advertising [370, 368]. However, other uses of phone numbers are also common and respective privacy and security implications have not yet received sufficient scrutiny. In order to investigate the privacy, security, and access risks associated with phone numbers, we identify five common uses of phone numbers by companies, each with varying levels of usefulness to users and benefit to companies.

Phone Number for Notifications. Online services and applications may use a phone number to send SMS alerts and notifications to users. Such alerts might be sent by online services or by businesses a person interacts with in the physical world (e.g., a doctor's office, apartment complexes, stores). For example, a pharmacy might offer to send customers an SMS when their prescription is ready [108], or airlines might alert a customer when their flight is delayed [12]. While such communication is often opt-in, SMS notifications can create a potentially sensitive leak of information. As with email [312], if these alerts were to go to the wrong person, for example after a number has been recycled, they could reveal a significant amount of personal information about the intended recipient and the intended recipient may miss important information.

Phone Number as an Identifier. Phone numbers are increasingly used as a way to identify and authenticate users in place of a username or email address. For example, loyalty programs frequently use phone number or email address to track purchases and rewards [228]. For some services, such as Twitter, users can opt to use a phone number rather than an email address to create an account [367]. In these cases, the user will typically need to verify that they own the phone number by receiving a phone call or SMS with a one-time code that they enter into the application or website. As noted above, the phone number may also be used in place of a password as the sole mechanism for proving ownership of an account.

Phone numbers are also valuable identifiers for companies wishing to perform targeted advertising or to connect profiling data across devices and sources. On platforms like Facebook, companies can upload lists of phone numbers in order to directly target those individuals with ads [133]. The common use of phone numbers across platforms means that companies may have a better chance of connecting and aggregating data from the same individual across multiple platforms and online spaces, compared to usernames which may or may not be consistently used. Much of this phone number use is done outside of the view of the user and therefore, such violations to privacy will be difficult for people to recognize. This use of phone numbers arguably offers little or no benefit to the affected users, but is profitable for companies.

Phone Numbers to Build Peer Networks. Phone numbers may also be used as a way to construct peer networks. For example, many mobile messengers like WhatsApp, Telegram, and Signal use phone numbers in place of usernames [385, 354, 338], which allows users to find each other on the platform if they know each others' phone numbers. This takes advantage of many people already having phone numbers of their friends, family, and colleagues saved in their phone's contacts, allowing a new app to construct a possible network of acquaintances by requesting access to the phone's contacts. For example, Facebook's People You May Know feature uses a user's phone number and uploaded contacts to suggest which other Facebook users to connect with [137]. This can be beneficial both for users, who can easily find other people on platforms, and for companies, who can profit from learning social networks. However, when companies *require* a phone number from all users and use it in this way, private personal connections can be unintentionally shared with a company — not only by the user, but by anyone who has their phone number stored in their contact list.

Phone Numbers for Account Security. Services may also ask users for their phone number to enhance account security. MFA can provide an extra layer of security to an account by preventing an attacker from logging into an account with a stolen or guessed password alone. While these one-time codes can be generated by a hardware token or sent via an app or email address, SMS remains a common medium for sending MFA codes to users, and is sometimes the only way for users to enable MFA.

Similarly, phone numbers are often used for account recovery [169, 135]. If a user has forgotten their password or lost access to an email address, access to the phone number that is associated with the account might be used as an indication that they are the rightful user of that account.

Phone Numbers as a Test of Uniqueness. A phone number is also sometimes used to prevent the same user from creating multiple accounts, or to limit the number of accounts per person. This mechanism relies on the assumption that having numerous phone numbers will be challenging for most users, as they may be expensive. Furthermore, in contrast to email addresses, which could be anonymous and which a user could have an unlimited number of, phone numbers are often connected to a person's legal identity. This restriction may also function as an accountability mechanism. If someone is banned from a platform, the need to obtain a different phone number might hamper their ability to rejoin the community under a different alias. For example, Facebook does not allow users to have multiple or fake identities on the platform, because they "believe that people are more accountable for their statements and actions when they use their authentic identities" [134]. Although Facebook enforces this policy using more information than phone numbers alone, they also prevent multiple accounts from using the same phone number [136].

Requiring a phone number to be associated with an account may also be used to reduce spam. For example, when creating a new account, Google asks the new user to "prove you're not a robot" by verifying their phone number via a text message or a call to their phone [171]. Google, like Facebook, also seems to limit the number of accounts per phone number [213, 98]. This restriction can benefit both users and the company, but when people are limited to only one account it may create barriers for people who have a legitimate need for multiple separate accounts, for example for professional and personal use or to represent different aspects of their identity.

4.2 Study Design

While phone numbers are collected and used in various ways, the potential negative consequences of these uses on people have not yet been studied systematically. In order to uncover the range of problems that people experience with phone numbers, including those that may be uncommon, we sought to elicit negative experiences with phone numbers from a large number of people. In this study, we do not seek to answer which problems are the most or least common, nor to measure how prevalent various problems are. Our objective is to qualitatively identify the different ways in which phone numbers and their uses create risk for people, what those risks are, and the consequences of those risks on people who have experienced them.

To meet these goals, we designed a concise, open-ended elicitation survey that we distributed widely. Using a survey as our elicitation instrument allowed us to ask a large number of people about their experiences, increasing our chance of hearing about issues that occur rarely and giving us a broader overview of problems than a smaller-scale interview study would have.

4.2.1 Experience Prompts

The survey consisted of four parts. The survey questions are provided in Appendix C.

Device and phone number ownership. We asked participants to indicate the type of their primary phone number (mobile, landline, or virtual), whether the number is theirs or shared with others, how often they have changed their phone number in the last 5 years, and how long they have had their primary phone number. Note that we did not ask for the actual phone number for privacy reasons.

Annoying, weird, or disturbing experiences. We next asked participants to describe any “annoying, weird, or disturbing experiences with phone numbers” in order to elicit whatever experiences were most salient to participants. This question was meant to ask for participants’ experiences surrounding their phone numbers without priming them about a specific type of issue. We did not further define or clarify these words in order to elicit any associations participants might have with phone numbers. We also asked about any consequences resulting from their experiences.

Specific experiences. Next, we asked whether they had experienced several specific issues, including inability to use an online service or app; losing access to a phone number; phone number recycling; discomfort with sharing their phone number; and any other negative experiences they would like to share. Again, we also asked for consequences from the experiences described. We asked about these specific experiences because we anticipated, based on the common phone number uses listed in Section 4.1.2, that they would frequently be events that led to negative consequences for individuals.

Demographics. Lastly, we collected participants' country of residence, age, gender, highest level of education, and employment status. Responses to these questions were optional.

We iteratively refined the survey order and content through pilot testing. We translated the survey into Spanish to expand the responses for international experiences. Our study went through the IRB approval process and was exempt.

4.2.1.1 Recruitment

To collect responses from a wide and diverse group of people, we shared the survey across multiple social media sites such as Facebook, Twitter, and Reddit between March and June 2019. In addition, the survey was shared to personal and professional networks and email lists at multiple universities. We further distributed the Spanish version within the local immigrant community and to personal networks in South America. The survey did not collect any identifying information such as phone numbers and all participants remained anonymous.

Participants could optionally enter into a raffle to win one of five $20 Amazon Gift Cards. Contact information for the raffle was stored separately from survey responses.

4.2.1.2 Demographics

We received 191 English and four Spanish responses. All Spanish responses were translated by the authors into English prior to analysis. Most of our participants lived in the United States with eight from Germany, and one each living in the Netherlands, Ireland, Guatemala, France, Colombia, Canada, and Australia. Participant demographics

Age	18-24	34
	25-34	89
	35-44	43
	45-54	9
	55-64	7
	65 or older	5
	Prefer not to answer	8
Education	High school graduate	3
	Some college but no degree	9
	Associate degree	1
	Bachelor's degree	51
	Graduate degree	116
	Professional degree	5
	Prefer not to answer	10
Employment	Employed full-time	102
	Employed part-time	11
	Student	59
	Self-employed	2
	Homemaker	1
	Retired	3
	Not working	6
	Prefer not to answer	11

Table 4.1: Participant demographics (n=195).

are summarized in Table 4.1.

4.2.1.3 Qualitative Analysis

After discarding empty responses, we used iterative, open coding followed by thematic analysis of the 972 open-text responses we received (7 open-response questions from 195 participants, some left blank). In line with the process described by Braun and Clarke [62], two researchers initially read the data and derived codes using participant language (e.g., “I don’t care”, “annoyed”) and descriptive terms based on the event described (“account lockout”, “changed number”). Codebooks were initially generated for each question, but we quickly observed heavy overlap across topics and combined them into one codebook (e.g., the question about phone number recycling contained descriptions of many of the other experiences we asked about). After an initial codeset was generated from these readings, two researchers discussed and merged overlapping codes, grouped similar codes into higher-level themes (e.g., “made up phone number” and “used old number” merged to “gave fake phone number”). We then tested the utility of the codebook on a subset of the data, adding new codes and merging further overlapping codes, with discussion, until no further changes were necessary, which required two rounds. The final codebook of 45 codes was applied to a subset of 15 responses with good inter-coder agreement (Cohen’s κ=.76) [258], after which all responses were recoded. The codes represent themes we describe in the rest of this work and closely align with the summary in Table 4.2.

Throughout the work, we quote our participants’ text responses. We removed or changed any identifying information (e.g., names), but we do not modify company names so as not to obscure the context of a described negative experience.

4.2.2 Limitations

Our goal with a qualitative elicitation study was to provide insight on the range of problems that people experience with phone numbers. Some of the experiences and consequences we discuss are difficult to capture. For example, interpersonal issues like harassment and stalking are among the most serious consequences of phone number exposure, but relatively few users might experience the worst forms of these harms or, even if they do, may not be willing to share such experiences.

Our sample is more highly educated than the general population, likely due to our recruitment method. This may mean that our participants, with more earning potential, are less likely to face issues that arise from prepaid phone numbers or inability to pay a phone bill. While six participants reported losing a phone number for financial reasons, research focusing on lower-income contexts might reveal additional nuanced consequences of this problem [244], in addition to the rich insights we report here.

While we do report the country of residence of participants, we did not ask our participants to specify where their experience took place. Some of the stories from U.S.-based participants happened internationally. Therefore, we do not make statements about phone issues in specific countries nor draw cross-cultural comparisons, but we also do not exclude any responses based on participant location. We did confirm that all themes reported by our non-U.S. participants were also reflected in similar U.S. experiences. In other words, none of our findings were based solely on non-U.S. responses.

4.3 Results

In general, most of our participants reported having minor issues with phone numbers that frustrate and inconvenience them; however, some shared experiences that created significant risk and had severe repercussions in their lives, demonstrating that collection and use of phone numbers can have real consequences on people. Our findings are summarized in Table 4.2.

While our sample does not allow us to comment on the frequency of problems in the general population, we indicate the prevalence of each problem among our participants.

4.3.1 Participants' Phone Number Use

When asked what type of phone numbers participants have had in the last five years, 191 of 195 participants indicated that they have a mobile phone number; 85 have a virtual number such as Google Voice or Skype number and 51 have a landline. 108 reported having two or more types of phone numbers. Only one respondent indicated that they share their mobile device with someone else (their spouse).

Almost half of our participants (91) have gotten a new phone number in the last five years, suggesting that phone numbers are less persistent than one might expect. 48 participants obtained a new number once in that time; 41 obtained new numbers 2–5 times. Most other participants (88) reported having their primary phone number for 10 or more years.

Negative experiences	#	
Loss of access to phone number	14	Loss due to international travel or move
	6	Loss due to unpaid mobile bill
	1	Loss due to SIM-swap attack
Phone number recycling	67	Must deal with the former owner's calls or text messages
	5	Harassed (e.g., by debt collectors)
	4	Gained personal information about the previous owner
	4	Contacted the wrong person when friend or family changed phone numbers
	3	Asked to relay messages to previous phone number owner
	3	Unable to use recycled number to register a new account
	1	Had personal information exposed to new owner of their old phone number
Companies sell or misuse data	140	Received spam (unwanted calls)
	23	Assumed companies collecting phone number would lead to spam
	19	Assumed companies would sell phone number
Interpersonal sharing	3	Feared dating websites would expose phone number
	1	Number exposed to someone through an app
	1	Phone number led to being found on another platform
Usability of phone numbers	3	Phone numbers are hard to remember
	2	International prefixes are confusing
	2	Changing phone numbers is burdensome
	1	Phone number looks like spam number to friends and family
Consequences		
Degraded utility	20	Wasted time
	18	Inconvenience
Erosion of trust in companies	21	Mistrust in companies asking for phone numbers
Emotional toll	80	Annoyed (e.g., at dealing with spam or other inconveniences)
	5	Felt physically unsafe
	1	Experienced significant panic and anxiety
Financial Loss	2	Needed to pay to change number
	1	Fell for financial scam
	1	Lost financial opportunity due to wasted time
Behavior changes		
Changing answering behavior	46	Stopped answering the phone or began ignoring unknown numbers
Correcting mistaken callers	17	Answered unknown numbers to tell caller the number was recycled
Sharing virtual or fake numbers	14	Gave companies or people fake numbers instead of real phone number
Blocking numbers	18	Routinely block numbers
	12	Use a call-blocking service
	2	Search unknown numbers online
	1	Report spam callers
Changing phone numbers	7	Changed phone number due to negative experience
Self-restricting behavior	22	Opted out of a service to avoid giving a phone number
	3	Used alternative service instead of sharing a phone number
Resignation	21	Shared a phone number when they did not want to
	10	Felt they had no choice but to share a phone number

Table 4.2: Summary of findings, with number of participants expressing each theme.

4.3.2 Negative Experiences

Broadly, we identified six types of negative experiences with phone numbers as reported by participants. The frequency of these problems, as well as the consequences, varied widely. For example, some experiences, such as problems with spam, were reported by nearly all participants but resulted largely in minor inconvenience, while other issues like harassment and concern about personal safety were mentioned less but had a significant impact on the respondent's life. We first present the types of negative experiences and then discuss resulting consequences and behavioral responses.

4.3.2.1 Losing access to a phone number

16 participants reported losing access to their phone number either temporarily or permanently. The most common reason was international travel or moving to another country. 14 participants reported having issues accessing a phone number or verifying an account while traveling or living internationally. This resulted in being locked out of financial applications, being unable to use their accounts, or needing to borrow family members' devices. P60 described, *"I lost my Chinese phone number [because] I forgot to pay my bill for several months. And it's very hard for me to get that back again... [T]o get the number back they require me to go to a service provider store in-person with my ID... so annoying... and this number is connected with many of my account[s] like my Alipay or WeChat. It's possible that this number would be registered by someone else if I don't get it back in a short time. I just don't know what to do in that case."*

For some users the lockout is not just temporary; accounts are permanently lost because users no longer have access to the phone number they used to register an account. P163 explained, *"My @126 email was linked to my old Chinese phone number which I cancelled. Now the first step to update that phone number is to receive a text validation code on that number on file. Which of course is impossible. Otherwise I need to go through a process to [prove] that I'm the owner with my ID or passport, which I feel is so unnecessary for an* *email. So I never updated that number."*

Several participants (6) reported losing access to a phone number because they were unable to pay the phone bill. Others had disputes with the service providers or changed numbers and were later unable to regain access to the old number when they needed to. Retrieving a phone number after it has been assigned to someone else is difficult, if not impossible. P20 described realizing that a deceased relative's phone number was the only method available to certain people for reaching their family after the number had already been recycled. When they could not retrieve it, they lost contact with those people.

Loss of access could also stem from an adversary. P194 described being the victim of a SIM-swapping attack: *"Someone went into a Verizon store in another city, showed a fake ID saying that they were my son, told the agent that they had lost their cell phone, and asked to have my son's cell phone number transferred to an old phone that they had brought into the store. We were lucky that my son noticed that his phone got a message that it was no longer 'authenticated' and that I knew what that might mean."* This participant was able to quickly regain control of the phone number and was able to stop the attack before any financial harm had occurred.

4.3.2.2 Phone number recycling

Many participants (72) have had negative experiences related to phone number recycling. Most commonly, they reported receiving a number that had been recycled and having to deal with receiving calls and messages intended for the number's previous owner (67). Others reported contacting the wrong person after a friend or family member changed their number (4). One person had their number reassigned to someone else.

For some participants, getting someone else's recycled number was simply an inconvenience. P170 wrote, *"[T]he last person who had [my] phone number didn't tell the majority of her contacts that she had switched phone numbers. ...the first couple years with my 'new' number were littered with random people texting/calling asking for her. This was funny at* *first and I even managed to pull a few pranks. But it became increasingly annoying as time went on. It has been 5 years with this number and I *still* get texts for her every once in a while."* Three participants even reported being contacted by the previous owner and asked to relay messages to them.

For others, dealing with someone else's number could be scary when the people calling for the previous owner did not believe it had been reassigned. Several participants (5) reported being harassed by debt collectors. Others experienced more personal attacks. P80 reported, *"I started receiving weekly collect calls from [a] Prison. Apparently the inmate's wife, ex-wife, girlfriend, or ex-girlfriend used to have my phone number. Even though there was an operator between us... I'd decline, yet I could hear the guy on the other end start screaming at me about stealing his woman, and threatening to hunt me down once he was out."*

Some participants even reported gaining access to the former owner's personal information when they received their new number. Four participants reported getting SMS notifications from businesses like banks and laundry services, or receiving birthday wishes from friends of the former owner. For each participant, this added up to a significant amount of information about their number's previous owner. In addition to the personal information, P105 reported having a "creepy" interaction with someone trying to contact the former owner: *"[T]he previous owner seemed does not change his contact info for bank services... I got messages regarding his bank transactions, had access to his [WhatsApp] account, received a dozen of phone calls from his friends looking for him, yet the most weird thing happened at one night — I was sleeping and hearing my phone ringing. it was a FaceTime call from an unknown Chinese number. ... I answered — there was a female's arm holding a baby and asked the baby to call daddy in a soft voice... it was midnight and that's just so creepy to me and I hung up the phone. She called several times afterwards and the following days. ... wonder what happened to [the former owner] as he seemed being away without notifying others about the change of his number."*

Conversely, one participant reported what happened to them when someone else was assigned their former phone number. P154 described discovering that their WhatsApp contacts had been talking to the wrong person after they had changed phone numbers. While only one person reported having their own information revealed by phone number recycling, several others expressed worry about what would be exposed about them if they eventually lost their phone number.

Phone number recycling can hinder access as well. Three participants reported being unable to create a new account with a company or sign up for rewards programs because the previous owner of the number had already created an account and had not yet changed the number. P24 shared, *"[I have] Maggie's phone number. I got her email address from groupme, can't open an uber account because the number is taken, have her birthday date because I got a happy birthday, got added to a whatsapp group..."*

4.3.2.3 Companies selling and misusing contact information

A large number of participants (74) described an experience in which they were uncomfortable sharing their phone number with a company or a person. For those who worry about sharing with a company, many of their concerns related directly to how companies used their phone numbers or how the participants expected their numbers would be used. The most frequently cited reason for discomfort was that participants assumed that companies would sell their phone number if they shared it with the company (19).

Even more participants (23) believed that sharing their phone number with too many companies would increase the amount of spam they receive. Sometimes a specific experience led them to this belief. For example, P191 described that they *"signed up for health care portal (obama care) to choose new health insurance. was bombarded with phone calls within minutes, for weeks and months to follow. still getting calls today, 2 years since."*

The concern about spam was significant. A majority of participants (140) complained about spam calls, such as calls from telemarketers, robocalls, or persistent unwanted calls of unknown providence. Of these respondents, nearly all brought up spam calls in the first question, which asked broadly about their experiences with phone numbers. This suggests that spam calls are a prominent issue in people's minds.

4.3.2.4 Distressing interpersonal disclosure

Potential interpersonal risks were another source of discomfort for some of our participants. Three participants said they dislike sharing their phone number with dating websites because they worry that the platform will expose their number to the people they connect with. P40 shared, *"[W]hen I have to use my number to log into dating apps, I worry that the app might give my number out to the other people on the app."*

Another participant (P157) described needing to share their phone number with a Grubhub delivery driver for their food order, but felt uncomfortable when the delivery driver *"tried to get personal."* In this case, the phone number had already been shared and the driver now had a direct line of access to the person they made uncomfortable.

Phone numbers, once shared, can open new avenues of contact that simple blocking cannot prevent because of the way that numbers are used across services. P97 described, *"There was also a time when some people were harassing me via text and then used my number to continue harassing me on WhatsApp with further information indicating that they'd doxxed me as well."* When phone numbers are used as identifiers across many platforms, they can help an attacker find alternative channels to harass or contact someone who has blocked them elsewhere.

4.3.2.5 Poor usability of phone numbers

Beyond negative experiences stemming from phone number use, several participants also complained about needing to use phone numbers at all. Three participants mentioned that phone numbers are hard to remember, two complained that international prefixes are confusing and difficult to use, and one reported being regularly ignored by friends and family because their area code begins with an "8" — leading their contacts to assume a telemarketer is calling. Several participants (2) also complained that updating all the services that have their phone number is burdensome if they want to get a new number, but that porting an old number to a new provider is also difficult.

4.3.3 Reported Consequences

The consequences that followed from the reported negative experiences with phone numbers varied in type and severity, ranging from annoyance and disruption to participants' lives, emotional ramifications like stress and fear, and even financial consequences. In total, these consequences demonstrate the real and sometimes significant impact problems like phone number recycling and phone numbers as user identifiers can have on people's lives.

4.3.3.1 Inconvenience and degraded utility of phones

Throughout our participants' experiences, many expressed their frustration at wasted time (20) and feeling inconvenienced (18) from dealing with their issues related to phone numbers. These feelings were most frequently associated with dealing with many spam calls or needing to answer calls for the former owner of their phone number.

When participants are locked out of accounts they had previously created because they cannot access their number, or are prevented from making new accounts with a recycled phone number, the convenience of using a phone number as an identifier is lost.

4.3.3.2 Erosion of trust in companies

Multiple participants (21) expressed a lack of trust towards companies or services who ask them to provide a phone number. Most frequently, participants connected this discomfort with a lack of understanding of why a company would ask them for this information. P187 wrote, *"I'm always uncomfortable sharing my phone number for no obvious reason (like why does Bath and Body Works care what my phone number is?) ...Unfortunately, I don't* *know what else to do, so I just bite the bullet and type in my phone number."*

Many other participants felt certain that companies would sell their phone number to other entities (19) and that sharing their number would result in more spam (23), and therefore did not want to provide their number. Unfortunately, as P187 expressed above, many felt they had no choice but to share their phone number. Many (21) described a specific situation in which they did not want to share their number, but did it because they had to. P121 described this frustrating trade-off: *"Telegram requires your telephone number as a user identifier. I was resistant at first, but eventually gave in. I don't like that this service has my number, but without the service, I would be unable to use it to speak with friends."*

4.3.3.3 Emotional toll

Many of our participants (71) expressed some emotional reaction to the experience they shared. The emotional reactions of our participants to their experiences varied from mild (e.g., annoyance) to extreme (e.g., fear).

Most commonly, participants expressed feeling annoyed about unwanted phone calls and text messages. But participants also shared harmful impacts and issues in their lives such as harassment and interpersonal problems.

Five participants shared experiences that made them feel physically unsafe. P158 described, *"One time several years ago, a man called my number in the middle of the night asking to speak to someone who was not me. I told him he had the wrong number. He called back and told me I sounded 'sexy,' that I should send him a nude photo, and that he knew where to find me. I told him I would call the police if he called back and I hung up the phone. He called back immediately but I did not answer and blocked the number."* P97 described being harassed and doxxed via SMS and then WhatsApp (see Section 4.3.2.4), which led to *"a metric f##kton of stress/anxiety"* and the decision to change residences.

While no participants specifically described physical harm being caused by these incidents, it is clear that the potential for such harm was present. Furthermore, the consequences of harassment itself can be long-term. For example, P196 described experiencing significant harassment over the phone that resulted in panic attacks whenever the phone rings, which was made worse by the increase in spam they began to receive. While cases of this severity may not be frequent, their existence demonstrates that significant emotional toll can be the price individuals pay for not having control over their phone number.

4.3.3.4 Financial loss

A few participants also described the financial cost of their experiences. P186 paid several thousand dollars for fraudulent car insurance as a result of a scam caller. Two participants described needing to pay fees to change phone numbers. P49 explained that they lose job opportunities and time (and consequently, money) every time they need to answer a spam phone call.

4.3.4 Behavioral Changes

Some participants found ways to cope or change their behavior in order to avoid the problems identified above. We found that many of these coping strategies in turn led to frustration or inconvenience for participants.

4.3.4.1 Changing call answering behavior

The most common way that people responded to unwanted calls was changing whether and how they answer the phone (46). This ranged from only answering calls from people they know to not answering at all and only relying on voice messages or text messages. Many participants speculate that in doing so, they have missed job opportunities, business calls, and medical appointments. P49 wrote, *"I have missed important phone calls and messages from potential jobs, and it's gotten so extensive I've contemplated paying the 40 dollar fee to change my phone number."* Similarly, P91 wrote, *"I don't pick up the phone for any phone number that's not in my contacts list anymore. If they want to get in touch* *with me, they can leave a message or email me."* Others simply silence their phone for all calls.

These strategies suggest that to cope with spam and unwanted calling, users are forced to adopt behaviors that undermine the original purpose of having a mobile phone.

4.3.4.2 Correcting mistaken callers

One laborious way in which people approached phone number recycling is correcting callers who are looking for the previous owner. 17 participants reported answering calls in order to tell others that they had reached the wrong person. While some had no trouble communicating the mistake to the person on the line, others expressed that this caused problems with the caller. P115 recalled, *"Yeah, one time someone called me when I lived in Oregon and asked to talk to someone who wasn't me. I said wrong number. She called back and then got annoyed at me, thinking I was playing a trick on her when I again said wrong number."* This echoes Rader and Munasinghe's findings on how people respond to and correct senders of manage misdirected email [312].

Two participants changed their voicemail message to clarify who they were to wrong number callers so that they would not have to pick up their phones anymore. According to our participants, correcting callers constantly constituted a waste of time and decreased the value of using a mobile phone. While some decided to completely stop answering their phones, others have to deal with correcting callers just to not miss a specific opportunity through phone calls.

4.3.4.3 Sharing virtual or fake numbers instead

When participants felt uncomfortable sharing their phone number, some ended up giving a fake phone number (4) or a virtual number (10) instead. P144 mentioned that the reason they don't worry about phone number sharing is that they are not afraid of giving out their Google Voice number. However, several participants mentioned that Google Voice numbers only work in certain apps or services. P168 described their strategy for using a fake number: *"In general, if I have to use a phone number for something, I have a regular 'fake' phone number I use that was a PAGER number I had when I was in college. I recognize that it could be recycled to other people, but I don't care. Everybody wants your phone number for marketing purposes and people who claim they don't give your number to anyone could be telling the truth since they SELL your number to other people...."* Participants are aware of the implications of sharing their phone numbers and look for ways to mitigate these issues through obfuscation, or adding fake information into a system meant to track them, thus disrupting the efficacy of the system [66]. However, in cases where the number needs to be usable, this will not work. Strategies such as changing phone numbers or using virtual numbers can also be costly and are not always available to everyone.

4.3.4.4 Blocking numbers or using call blocking services

18 participants described blocking numbers directly and 12 used some type of call blocking service, such as opting into the FTC's Do Not Call registry [97] or using call blocking apps like Mr. Number [192]. However, many of the participants who use these services claimed that this strategy is futile. P30 wrote, *"My efforts to block them don't work because they end up changing the number."* P119 wrote, *"My number is on the Do Not Call List, but it doesn't seem to matter. Recently I've been getting 2-3 per day"*.

Two participants said they research any unfamiliar phone numbers (P18, P110), while P92 actively reports phone numbers (though they did not specify to whom).

4.3.4.5 Changing phone numbers

Only seven participants reported changing their numbers due to their negative experiences. P102 explained how their child had received a phone number that was formerly used by a drug dealer and sought to change the number. They complained that the service provider insisted on charging them to change the number, but eventually provided a new number for free. P49, despite receiving many spam calls, contemplated paying to change the number but had not done so. Specifically, four participants were concerned with the costs of changing numbers, with one participant claiming it would cost them $40 to change their phone number. Moreover, as phone numbers are increasingly used as identifiers for accounts, the time required to update all of one's accounts and services with a new phone number can be burdensome and thus be a further deterrent to changing numbers. P105 mentioned, *"I was thinking to change a phone number but then I need to update a lot info that associated with this phone number, it's kind of troublesome so I haven't changed it yet."*

4.3.4.6 Self-restricting behavior

22 participants opted not to use a particular service or app because they either could not provide a valid phone number or felt too uncomfortable to share their phone number. Only three participants described being able to find an alternative service. P59 reflected, *"More than once I've been asked to provide a phone number before proceeding. In some cases this is jawboning, trying to make me provide my phone number, but caving when I refuse. In other cases, I can't move forward, so I don't."* P7 expressed that it is becoming more difficult to find alternative services that won't ask for a phone number. This shows that for certain services or apps, participants are being forced to choose between participating or restricting their usage just to preserve their privacy.

4.3.4.7 Resignation

While six participants expressed that they do not engage in any specific strategies to avoid these negative experiences, 21 participants reported that when prompted to share a number they didn't want to share, they surrendered and provided their phone number anyway. 10 participants felt as if they could not do anything but share their phone number if they want to receive a particular service, which reflects other work showing "digital resignation" as the inevitable result of consumer surveillance practices [124]. P95 stated, *"It is usually required for most things online, even when it seems unnecessary. I would prefer to not share this info but it seems mandatory to receive services online."*

4.4 Discussion

The proliferation of phone numbers in commercial and social contexts, often with companies facilitating the exchange while collecting and processing the data, has led to significant costs to users. Our findings characterize the many problems individuals have with phone numbers, and highlight that the associated costs to them can be significant. In particular, we discuss how companies that use phone numbers as user identifiers make implicit assumptions about users that lead to some of these issues. We then discuss the implications for tech platforms and policy considerations.

4.4.1 Issues from Faulty Assumptions about Phone Numbers

As discussed in Section 4.1.2, the uses of phone numbers by companies can serve a wide range of purposes. However, our results illuminate that many of the problems users face with their phone number also stem from these common uses. Here, we highlight how the use of phone numbers as identifiers by companies in particular creates challenges for individuals. Our findings show that the implicit assumptions by companies that phone numbers are *persistent* and *unique*, that a phone number is consistently *available* for authentication and account use, and that people are *comfortable* sharing their phone number with a company and possibly with other users, are flawed.

Phone numbers might not be unique or persistent. While many services operate assuming that a phone number will persistently belong to one user, people can and do change phone numbers; indeed, almost half of our participants had gotten a new number in the last 5 years. When people forget or are unable to update their phone number, this may result in missed notifications, login problems, account lockouts, or private information being sent to the wrong person.

Furthermore, not all users have a unique phone number or device to begin with. Although only one of our participants shares a phone number with a spouse, this is likely a larger issue internationally in places where sharing devices is more common [10]. Shared devices may cause additional problems when multiple accounts cannot be associated with the same number, or if a login can be processed through a verification code sent via SMS rather than a username and password, allowing a different user of the device to log in against the wishes of the account holder.

Phone numbers are not always available. Even when people are willing or required to provide their phone number, the mobile network may not be consistently available. As shown by our participants, people may be unable to pay their phone bill, may travel or move internationally, or otherwise lose access to a phone number temporarily or permanently. 14 of our participants reported issues with account access due to international travel or living, causing problems from inconvenience to complete and permanent inaccess. Potentially worse, phone number recycling means that recovery codes might be delivered to the wrong person, providing them with information that could be used to hijack an account. In either case, the use of a phone number as a way to authenticate or recover an account can create costly barriers, which may be especially frustrating in cases where the phone number itself is not necessary to provide the service.

Sharing can give unwanted intimate access. In the previous cases, problems arise when a number cannot reliably identify or authenticate someone over time. In other cases, a phone number *being* a persistent personal identifier—and shared inappropriately—is the issue. Phone numbers directly provide the ability to contact an individual, regardless of the context or reason the phone number was provided. As is well documented, Facebook's People You May Know (PYMK) feature has been shown to cause a number of similar issues to the ones we identify here. PYMK opportunistically suggests friends based on information Facebook collects about users, including phone numbers [137]. This can be a problem for someone who uses a phone number in multiple contexts. For example, sex workers who work under an alias to protect their identity may see clients being suggested as friends on Facebook, despite taking extra precautions otherwise to keep work and personal accounts separate [190].

Phone number use in the mobile messaging ecosystem can also be especially risky for certain users. Many mobile messengers, such as WhatsApp and Signal, display a user's phone number to everyone that person chats with. A protest group using WhatsApp to communicate not only exposes all members of the group to one another, but also to anyone who confiscates a member's device or infiltrates the group. This is exactly what happened in March 2020, when the Lebanese Government reportedly used WhatsApp groups to infiltrate the social networks of protesters and track them based on phone numbers [22, 223]. Once a phone number is in the hands of an adversarial government agency, it can be used to physically find and track the owner with a cell-site simulator, as has been done by the U.S. Immigration and Customs Enforcement to find and deport immigrants [343].

4.4.2 A Public Number Becomes Private

Phone numbers by design were meant to be shared; they were commonly available in phone books to facilitate easy contact for friends and neighbors [308]. Now, phone numbers are becoming increasingly guarded. In this way the phone number has followed a similar trajectory to the American Social Security Number (SSN). As described by historian Sarah Igo, when introduced in the 1930s, SSNs were controversial; meant to facilitate the collection, and later disbursement, of financial benefits for workers, some skeptics feared they were the beginning of a national identity system. As the system gained traction and some critical number of Americans opted in, those who were left without this number began to be locked out of job opportunities. Those who had been assigned a number might even show it off publicly, for example by having it engraved on jewelry or even tattooed onto their bodies [200].

As with phone numbers, private companies began using SSNs for their own bookkeeping, making them more valuable for more purposes. Soon this number was no longer so comfortably shared, and today SSNs are carefully guarded because they can be used for identity theft, allowing an attacker to open credit cards, access government benefits, and wreak other havoc on one's financial life [8, 206]. Similarly, we found our participants carefully guard their phone numbers, worrying about the information being sold or exposed to scammers by companies, exposing private information about them, or giving an attacker access to their online accounts.

4.4.3 Disclosing Phone Numbers Should be Optional

As we explored in Section 4.3.3, the cost to users of the prolific ways phone numbers are currently used is hardly negligible. To various degrees, users are facing degradation of utility, financial harms, loss of trust in companies, and emotional and safety consequences in dealing with problems stemming from the overexposure of their phone numbers. Some of these issues can be considered a problem of context collapse [246] — phone numbers shared in one context with one intention create pathways to expose information in unexpected ways and contexts.

We argue that companies should stop requiring users to connect a phone number to their account when at all possible. In many cases, a service can be run with an email or username rather than a phone number. Users should have the option to choose their preferred identifier based on their own privacy needs. Furthermore, in any application that does collect a phone number, that number should *never* be exposed to other users unless explicitly done by the user. More generally, the way a company plans to use a phone number should be clearly communicated to users and any additional uses after the number has been provided should be strictly opt-in.

4.4.4 Phone Numbers are a Risky Authentication Method

While SMS-based authentication may be easy and cheap to deploy, the likelihood that a phone number will not persistently belong to the same person, for example because of the high rates of phone number recycling, impairs the utility of phone numbers for security purposes. After a number is reassigned, the wrong person could receive MFA or login codes, allowing them to gain access to another's accounts. As one of our participants experienced, a determined attacker might even be able to hijack a *particular* user's phone number through SIM-swapping. Only one of our participants experienced this, but a recent study by Lee et al. found that of the five U.S. mobile service providers they tested, they were able to successfully perform a SIM-swap at all five, showing that the attack is easily achievable for a minimally informed attacker [232].

These attacks, especially when targeted to specific high-value users, can have significant consequences. For example, Twitter CEO Jack Dorsey had his Twitter account taken over by an attacker who proceeded to fill his account with offensive messages, harming the CEO's and the company's reputation [61]. These attacks can have financial consequences too, and have been used to steal hundreds of thousands of dollars worth of cryptocurrency from online wallets [306]. That SIM-swapping is such a lucrative attack demonstrates that having access to someone's calls and texts can provide access to a slew of sensitive accounts. As an additional risk, the mobile networks that transmit calls and SMS messages are themselves insecure [310], enabling untrusted entities and even enterprising individuals to eavesdrop on legitimate calls and texts without compromising any individual's accounts or mobile device.

In this way, our findings bolster other recent calls to deprecate SMS-based MFA [176, 266, 336]. While phone numbers for MFA and account recovery may still be useful in supplementing other account security mechanisms, the high cost of a phone-based attack should drive companies to consider making more robust security mechanisms, such as software- or hardware-based MFA tokens [122], a priority. Companies should further encourage users to opt for non-phone number based mechanisms as the default.

4.4.5 Mitigate Effects of Phone Number Recycling

Many of the most common issues reported by participants with phone numbers being used as user identifiers arise when they change phone numbers. These issues range from being locked out of accounts, getting unwanted calls for the previous owner, and being at risk for privacy exposures.

Because unwanted calls are a significant consumer complaint, the FCC has recently taken steps to address phone number recycling. In December 2018, the FCC imposed that phone carriers must wait a minimum of 45 days before returning a previously used number into circulation — a wait that was previously mere days — and introduced plans for a centralized recycled phone number database [139]. This database would be a list of all recently released phone numbers that companies will be able to query to learn whether the phone number they're trying to contact has been released and reassigned since it was provided to them. We suggest that similar information should be made available to consumers when they receive a new phone number.

Nevertheless, with this approach phone numbers will continue to be recirculated shortly after being released and the onus is on services to use the database to protect consumers. At this point it is unclear how effective this will be at reducing unwanted calls and preventing account creation problems for people who receive a recycled phone number. Additionally, such a database certainly raises several privacy and security concerns in itself, for example by creating a list of recently relinquished phone numbers for an attacker to use to authenticate to different services.

We argue that a more decisive solution is warranted. Scarcity of phone numbers is artificial. Phone service providers and regulators should expand the space of possible phone numbers to a size that significantly reduces the chance of phone numbers being recycled, or that allows for a significantly longer decommissioning of phone numbers between users. For instance, other countries (e.g., Germany) use 4- or 5-digit area codes, whereas the U.S. uses 3-digit area codes. This may be inevitable anyway; the North American Numbering Plan Administrator (NANPA), which controls the allocation of phone numbers in most of North America, projects that the current space of 10-digit numbers will be exhausted by 2049 [9]. Given the significant problems that are already arising with phone number recycling, we recommend this change be seriously and quickly considered.

4.4.6 Enable Contextualized Use of Phone Numbers

The measures that participants can and are taking to deal with the consequences of phone number (mis)use are insufficient to solve the problems created by having their phone numbers prolifically used in online accounts and applications. Steps such as permanently silencing phones, giving out fake numbers, opting out of using wanted services, or simply resigning themselves to being exposed are all annoying and disruptive to people, and ultimately ineffective.

Although in many cases phone numbers should *not* be required for identification, in the cases where this remains necessary or convenient to users, people should be able to easily and comfortably share a number they don't worry about being connected to the wrong part of their online identity. An excellent example of this is Apple's "Hide My Email" feature, in which Apple generates a unique email address that's associated with the user's account when they use Sign-In with Apple [31], effectively hiding the user's real email from third-party services. We recommend that phone service providers and regulators work to make it possible for consumers to have multiple phone numbers associated with the same SIM card or device in a similar way. This process has started somewhat: phone manufacturers have begun releasing phones with two SIM card slots or the capability to manage two phone numbers virtually [168, 32]. However, these specifications are designed for managing two numbers. In the ideal world, a user should be able to share a different phone number with their Uber driver than they use on a dating website, or list on LinkedIn, or use for personal communication with friends and family.

While this does not eliminate all problems, this could relieve some of the anxiety that our participants expressed over having to give out their phone number, while retaining many qualities that make phone numbers useful as account identifiers for companies. Similar to how security experts recommend people to have a different password for each online account to prevent many accounts from being compromised if one site experiences a breach [320], a different phone number for different areas of one's life may give a person more control over how and where their identities are connected online.

However, this recommendation may be ideal only in the short term; as we heard from participants, the format of a phone number is also not user-friendly. A significant increase in the number of phone numbers each person has to remember and use risks complicating online identity management rather than relieving it. Similar to efforts aimed at eliminating the need for passwords [53], future work should consider a future without phone numbers as identifiers at all in favor of more flexible, usable methods of identification.

4.5 Conclusion

Phone numbers are intimately connected to our online and offline lives. Our online elicitation study with 195 phone users yielded qualitative insights into the range of negative experiences connected to the way phone numbers are used. We find that people struggle with phone number recycling, loss of access to their number, and deal with privacy concerns. We also find that people experience significant harms following these issues, including harassment, account access issues, and eroded trust in companies, which lead people to adopt inconvenient and largely ineffective coping strategies. Based on our findings we discuss how faulty assumptions made by companies in their use of phone numbers as user identifiers lead to inflexible and sometimes harmful design decisions, and how companies and regulators should step in to provide better protections against privacy harms from phone number use online.

Ultimately, while individuals might be able to take small steps to protect themselves, the ability to make the best decisions for themselves is severely limited by the decisions companies are making about how to collect and use phone numbers. People use phones and their phone numbers in so many different ways — not every person will have a phone number that is uniquely theirs across space and time, that corresponds to all parts of their online identity. It is the joint responsibility of companies, regulators, and researchers to find the way forward for online account management that is safe and feasible for all people.

CHAPTER V

403 Forbidden: Global Disparate Access to Content via Geoblocking[1]

Harm does not only come to people through user-facing platforms. The design decisions and policies of companies involved in the core infrastructure of the Internet can also create or enable harms through the tools and features they provide to their own customers. In this chapter, I discuss a large-scale investigation of one of these features, provided by hosting providers and web content delivery networks, which enables websites to significantly limit access to information for large groups of people.

Researchers have devoted significant effort to measuring and circumventing nation-state Internet censorship (e.g., [397, 143, 290]). However, censorship is not the only reason why online content may be unavailable in particular countries. Service operators and publishers sometimes deny access themselves, server-side, to clients from certain locations. This style of geographic restriction, termed *geoblocking* [363], may be applied to comply with international regulations, local legal requirements, or licensing restrictions, to enforce market segmentation, or to prevent abuse.

[1] This chapter is based on: Allison McDonald, Matt Bernhard, Luke Valenta, Benjamin VanderSloot, Will Scott, Nick Sullivan, J. Alex Halderman, Roya Ensafi. 2018. 403 Forbidden: A Global View of CDN Geoblocking. In Proceedings of the Internet Measurement Conference 2018 (IMC '18). [252]
This work was supported by the National Science Foundation under grants CNS-1409505, CNS-1518888, and CNS-1755841. We are also grateful to Cloudflare for providing data.

Geoblocking has drawn increasing scrutiny from policymakers. A 2013 study by the Australian parliament concluded that geoblocking forces Australians to pay higher prices and should be regulated [36], and in 2017, the European Union banned some forms of geoblocking in order to foster a single European market [101]. Moreover, some Internet freedom advocates argue that the harm posed by geoblocking extends beyond the financial: it contributes to the wider phenomenon of Internet "balkanization" [111], in which users from different regions have access to vastly different online experiences.

Although some instances of geoblocking may be justified, there is abundant anecdotal evidence that overblocking frequently occurs. For example, after the GDPR came into effect in May 2018, several major U.S.-based news sites blocked access from Europe entirely [41]. All sites built on Google App Engine are unavailable in Cuba and Iran, due to Google's interpretation of U.S. regulations [390]. Other companies block all users from regions that produce large volumes of abuse, such as comment spam, when alternative security measures might result in far less collateral damage [356]. We hope that quantifying geoblocking will help reduce such overblocking by highlighting the extent of its impact on users globally.

In this work, we report the first global measurement study of website geoblocking. Comprehensively measuring geoblocking is challenging. The phenomenon takes many forms: sometimes a whole website is blocked in entire countries, while in other instances only particular content items are unavailable. In many cases a site is reachable but refuses to accept payment from or ship goods to users in blocked regions. Services often do not disclose that they practice geoblocking, so the reason content is unavailable must be inferred and distinguished from other anti-abuse practices and from network-based censorship.

To make large-scale measurement tractable, we focus our investigation on one important means by which sites implement geographic restrictions: using features built into large CDNs and cloud providers. Many popular providers, such as Akamai and Cloudflare, allow sites to restrict their availability by country. Using these CDNs, we positively identify specific characteristics associated with services enabling geographic controls, and use those characteristics to identify a larger set of CDNs that enable customers to geoblock. Within a large set of popular sites, this allows us to characterize the types of content that are most likely to be unavailable and the places where unavailability can be attributed to legal requirements.

To measure the extent of CDN-based geoblocking worldwide, we used Luminati [243], a commercial platform that sells access to proxy servers operated by users of the Hola VPN service. To safeguard those users, we refrained from probing sites from high-risk categories as well as sites known to be censored by governments. (We discuss these and other safeguards and ethical considerations in Section 5.2.3.) We implemented a new probing tool, Lumscan, that greatly improves the reliability of the data.

We collected two principal data sets. First, we developed a semi-automated system for identifying geoblocking enacted through CDNs. We accessed a safe subset of the Alexa Top 10K sites from 177 countries globally, extracted and clustered possible block pages, and manually examined each cluster. From this, we identified 7 CDNs and cloud providers that facilitate widespread geoblocking and extracted signatures to recognize each blocking behavior. Next, we found the customers of these CDNs in the Alexa Top 1M, took a 5% sample of these domains, and tested them globally to find the relative rate of geoblocking of each of these CDNs customer sets.

Our results show that geoblocking is a widespread phenomenon, present in most countries globally. Of the 8,000 Alexa Top 10K domains we tested globally, we observed a median of 3 domains inaccessible due to geoblocking per country, with a maximum of 71 domains blocked in Syria. Of domains in the Alexa Top Million, we observed an overall rate of 4.4% of domains utilizing their CDN's geoblocking feature in at least one country. We observed countries that are currently under sanctions (Iran, Cuba, Syria, and Sudan) to be geoblocked at a significantly higher rate, and Shopping websites to be the most common type of service to geoblock by raw number of domains.

Beyond characterizing CDN-based geoblocking, our results show that server-side blocking can be a significant source of error for censorship measurement—an area of very active research (e.g., [397, 290, 153]). We find that 9% of domains on the Citizen Lab Block List [88], a widely used list of censored domains, returned a CDN block page in at least one country. This indicates that censorship measurement studies should take geoblocking into consideration before ascribing unavailable sites to network-based censorship. We also discuss the relationship between censorship and geoblocking.

Roadmap: Section 5.1 provides background on geoblocking and our methodology. Section 5.2 describes exploratory measurements that informed our study design. We report our Alexa Top 10K measurements in Section 5.3. Section 5.4 expands our investigation of the CDNs identified in Section 5.3 into the Alexa Top 1M. Section 5.5 reveals data provided to us by Cloudflare and validates our previous observations. Our discussion of the relationship between censorship and geoblocking, the role of CDNs, and our limitations can be found in Section 5.6. Section 5.7 reviews related work, and we conclude in Section 5.8.

5.1 Background

5.1.1 Geoblocking

Websites may choose to restrict access to their content for many reasons. On forums seeking instructions for blocking Internet traffic by country (e.g., [378]), we see motivations that range from complying with legal restrictions, removing access from locations with many malicious login attempts, or simply reducing unwanted traffic.

Legal restrictions are an often cited reason that websites geoblock. U.S. export controls, managed by the Office of Foreign Asset Controls within the Department of the Treasury, limit both physical and intellectual property that U.S.-based entities can transfer to some nationalities without explicit authorization [116]. Similar institutions exist in many countries to enforce international sanctions and tariffs, and many websites may feel compelled to deny access because of embargoes. There can be significant unintended consequences to such broad enforcement of export restrictions.

Geoblocking can present itself in many ways. A website may choose to entirely block the network connection, resulting in timeouts when trying to access the site. Other sites might serve a custom block page that explains why access has been denied. Geoblocking may also happen at the application layer. A user may be able to load the main page of a website, but find that the login button has disappeared, or that some content is not available. These more nuanced changes in content are of significant interest, but we leave these questions to future work. In this work, we focus on detecting when websites entirely deny access.

From the user's perspective, whole-site geoblocking will sometimes present itself as an HTTP status code `403`. This status code is defined in RFC 7231 as a tool for a server to inform the requester that it "understood the request but refuses to authorize it" [142]. Because some service denial occurs due to international sanctions, the HTTP status code 451 is also relevant. Defined in RFC 7725, this status code is intended to inform users that their request was denied for legal or policy reasons [63]. However, this status code has not yet seen wide adoption, and we only observed an HTTP 451 twice in the course of our experiments.

Content Delivery Networks (CDNs) will commonly provide customers with security control tools. With these, customers can block IPs or locations based on their own policies or using a reputation score of the request or IP, which, for example, might be calculated based on rate of HTTP requests from a particular client (e.g. DoS protections) [14]. In these cases, a user will receive a block page that has been generated by the CDN rather than the end server.

While private companies are free to restrict access to content as they see fit—and are sometimes legally required to do so—our interest in this phenomenon stems from wondering to what extent geoblocking is contributing to the fragmentation of access to content online, which can be detrimental to the participation of Internet users worldwide in the global online community. We hope that by shedding light on the scope and impact of geoblocking, we can induce companies and policymakers to more fully consider alternative methods for meeting regulatory and security needs that cause less exclusion of users online.

5.1.2 Methods of Data Collection

Collecting representative measurements of site availability is a long-standing challenge in the field of censorship measurement. We want to both know that our measurement method is diverse enough to capture the phenomenon across a region and, in the case of censorship measurement, that if a user is associated with the device conducting the measurement, they are not put in harm's way because of sensitive domains being requested from their device. Fortunately, this second consideration is one way in which our study differentiates from censorship measurement—we wish to see when servers refuse access to a user, not when a nation-state blocks access. This allows some additional flexibility in measurement technique, as discussed below.

We collected measurements from a range of vantage points in different locations and across types of networks. Our primary vantage points were residential user machines provided through the Luminati proxy service. Luminati leverages the user-base of Hola Unblocker [194] for client-based proxy nodes. Luminati users connect to a superproxy with configuration information, including the desired geographic location of an exit node, whether to use the same exit node for multiple requests, and whether to send traffic via HTTP or HTTPS. Our use of Luminati follows the characterization of the service presented by Chung et al. [87].

For validation process, we also used a set of VPSes in 16 selected countries. We selected 9 servers to span the GDP range of country wealth by selecting every 10th country down a list of relative GDP [202] until it was difficult to find legitimate VPS services. We selected an additional 7 countries based on researcher interest due to known sanctions or reputations for content unavailability. The 16 VPSes were located in Iran, Israel, Turkey, Russia, Cambodia, Switzerland, Austria, Belarus, Latvia, the United States, Canada, Brazil, Nigeria, Egypt, Kenya, and New Zealand.

The VPS providers we used were based on recommendations from local activists. We did not use certain popular VPN/VPS providers because of their malicious marketing strategies: Ikram et al. [201] observed that some VPN providers such as HideMyAss and SecureLine often manipulate their WHOIS records to influence how their vantage points are geolocated by third parties. We verified the location of each VPS by requesting a website we set up on Cloudflare, and examining the geolocational headers Cloudflare inserts. This gives us some confidence that the claimed location of each VPS is likely to match the data CDNs use in making geoblocking determinations.

5.2 Exploration and Validation

For our initial exploration of geoblocking, we identified two services that offer geoblocking as a feature, Akamai and Cloudflare. Akamai's Content Delivery Network is one of the world's largest distributed computing platforms, with more than 233,000 servers in over 130 countries, peering with over 1,600 networks around the world. Cloudflare is another global CDN, with numerous connections to Internet exchange points worldwide [92]. These two CDNs combined provide services to more than 25,000 of the Alexa Top Million domains, and in total multiple millions of domains [68]. Since these CDNs make it easy to implement geoblocking, we reasoned that many of their customers likely enable it, making them ideal candidates for our exploratory measurements.

5.2.1 Identifying and Validating Signals of Geoblocking

We identified a subset of Alexa Top Million that are customers of Akamai and Cloudflare by examining the DNS server used by each domain. While this method only exposes a fraction of Akamai and Cloudflare customers, it gives us a subset of domains we can be confident use Akamai and Cloudflare. In all, we found 2,171 domains using Cloudflare and 4,111 using Akamai.

Fetching each of these domains from a VPS in Iran using `curl`, we observed 707 HTTP `403 Forbidden` responses, compared to 69 from a U.S.-based control server. Upon inspecting these pages in a browser, we found that both Akamai and Cloudflare present easily recognizable error pages that make them differentiable from other forms of blocking, such as block pages generated by Internet censorship in Iran [34]. It is important to note that the Cloudflare page specifically indicates that it is being served due to geoblocking, but the Akamai page is less specific and also appears when Akamai's abuse detection system is triggered.

To scale up these measurements, we used ZGrab [127] from our set of VPSes. We first validated the behavior of ZGrab by randomly selecting 50 domains and manually observing that the response received when requesting the home page through ZGrab was the same as when the home page was loaded interactively in a web browser set to use our VPS as a proxy. ZGrab was configured with the `User-Agent` string set to mimic Firefox on Mac OS X. We manually checked all responses returning status code 403 observed in Iran, Turkey, Israel, and the U.S. to confirm that the same status was returned when collected in a real web browser. We found that on the order of 30% of the Akamai 403s appeared to be false positives: the crawler request was flagged as a bot or otherwise was denied access while a real web browser request was able to load the page. The set of domains that resulted in false positives from ZGrab were nearly identical across countries, indicating that these false positives are not typically location dependent.

Next, we fetched the 6,282 Cloudflare and Akamai domains in the Alexa Top 1M from each VPS (100,512 domain-country pairs) and detected 1,068 domain-country pairs that resulted in block pages (19 for Cloudflare, 1,049 for Akamai). Once again, we manually verified each block page instance by visiting it in a web browser tunneled through the VPS. Of the 1,068 instances, 782 appeared to be genuine instances of geoblocking (19 for Cloudflare, 763 for Akamai), with 269 unique domains in total (12 for Cloudflare, 257 for Akamai).

Of the 1,068 instances of likely geoblocking across all domain and country pairs initially reported by our automated data classifier, 286 (27%) proved to be false positives upon manual inspection—all from Akamai.

5.2.2 Lumscan: Luminati Scanning Tool

The Luminati service is a collection of HTTP proxies that exit traffic at residential machines, enabling us to make requests from an end-users' vantage points within each country. However, Luminati is not perfect; since the residential IPs are VPN users, interference by the local network can be expected on those clients' requests. In order to overcome the challenges associated with getting raw data from an end-user connection, we developed a tool, Lumscan, to perform our measurements with a number of features to improve the reliability of our results.

The first improvement Lumscan performs is to verify connection to a known online page, in order to verify that the client has local web connectivity. We connect to a Luminati-controlled webpage that also returns the client's IP and geolocation information. Second, Lumscan repeats each failed request a configurable number of times. This reduces the impact of proxies on unreliable networks.

Lumscan also allows the user to specify HTTP headers that are sent in the final request. Merely setting `User-Agent` is insufficient to suppress bot detection, which likely contributed to the high false positive rate in our VPS study.

Finally, in order to support a high rate of requests, we implemented load balancing. We distribute requests across residential exit machines as well as across the Luminati superproxies that mediate our requests. We only perform 10 requests with a given exit machine before changing exit machine. This keeps us from consuming too many resources on any single end user's machine. It also allowed us to collect each of these datasets in a matter of hours rather than days, providing a single snapshot in time and minimizing the chance of observing policy changes.

5.2.3 Ethics

Our initial investigation of geoblocking used 16 vantage points in different geographic regions, all located in commercial hosting facilities. In all cases, the account for the server used an author's real name and university email address, and we complied with the terms of service and acceptable use policies of the hosting companies. This allowed us to probe availability of a broad range of content without imposing risks on end users.

Our broader data collection from residential IPs made use of the Luminati VPN service [243]. Luminati allows paid traffic to exit the computers of end-users who have installed their free VPN service. Luminati advertises itself as allowing competitive market research, but the company was supportive of our research during multiple Skype conversations.

In order to reduce the risk that our research would not negatively impact the Luminati end users, we carefully limited the set of sites that we probed. We removed several categories of sites: pornography, weapons, spam, and malicious content, as well as any sites that were uncategorized. We also removed domains that had been identified as censored by Citizen Lab [88].

We did not collect any personally identifiable information about Luminati users. Each probe result contained the geolocation information provided by Luminati and the HTTP and HTML data returned by the web request. Although Luminati returned IP addresses of the exit nodes within the geolocation information, we discarded these before doing any analysis on the data. As such, our IRB determined that the study was outside its regulatory purview.

5.3 Alexa Top 10K

Our early exploration gave us an insight into how two specific CDNs, Akamai and Cloudflare, allow their customers to geoblock. We want to now expand our understanding of the phenomenon across additional CDNs, as well as investigate whether we can observe

Initial Domains	Safe Domains	Initial Samples	Clustered Pages	Clusters	CDNs & Hosting Providers
10,000	8,003	1,416,531	24,381	119	7

Table 5.1: Overview of data at each step in Methods. This table shows the data at each step of our geoblock page discovery process. "Initial Samples" consists of the 3 samples per domain in each of the 177 countries we examine.

other instances of geoblocking, potentially implemented in other ways. To do this, we explore geoblocking across the Alexa Top 10K most popular domains across 177 countries.

5.3.1 Methods

Our data was collected using our Lumscan tool with the Luminati Network. We extract possible block pages from our dataset, cluster them, and find new block pages. We then search the dataset for instances of these block pages and sample the domains again in countries where we saw them, in order to increase confidence in our observation. This methodology is described in more detail in this section, and a summary can be found in Table 5.1.

5.3.1.1 Initial Dataset

We choose to study the Alexa Top 10K domains as a set of popular websites with a global reach. Because we are requesting these domains from end-user devices, we first classify the 10,000 domains using FortiGuard and remove any dangerous or sensitive categories, such as Pornography, Weapons, and Spam. We also remove any domains that appear in any of the Citizen Lab censorship list for any country. This leaves us with 8,003 domains.

We began by sampling from 195 countries and kept countries that were able to respond to all of our requests. Each domain is sampled 3 times as a baseline measurement. 177 countries were able to respond to all our requests.

Overall, we observe 286 domains that never successfully respond to our request. Luminati itself blocks requests to some domains, which can be identified with the header

X-Luminati-Error. These account for 13 of the inaccessible domains. The rest of the requests consistently timed out or tried to make more than our limit of 10 redirects. 90% of the domains we sampled saw less than a 11.7% error rate, where error indicates that we were unable to get a response from the site, either due to proxy errors or errors such as timeouts and lengthy redirect chains.

The errors are also not inordinately affecting only certain countries. From our initial 3 samples per country-domain, we have at least one valid response from between 89.2% and 93.9% of tested domains in each country. The one exception to this, Comoros, sees a response rate of 76.4%. This shows that an initial snapshot of 3 samples per country-domain pair gives us excellent coverage of domains in nearly every country.

5.3.1.2 Metrics for Identifying Outliers

From these samples, we want to extract pages that are likely block pages. Guided by the work of Jones, et al., we first explored whether page length is a good metric for finding outlier pages [211]. For each domain, we extract the longest observed instance of the page across countries and note that length as the likely size of the true page. We then compare the size of each individual sample for a domain to the representative size. If the length difference is greater than 30%, we extract this page as a possible block page for clustering.

However, we found that we were collecting enough data that potential block pages were too many to be clustered efficiently. In an early exploratory experiment, we had taken our list of Akamai and Cloudflare domains used in our VPS study to sample each domain 10 times in every country and ranked the countries by number of Akamai and Cloudflare block pages seen. With information from this data, we take the top 20 countries with the most block pages and find the representative sizes in our Alexa 10K data among those countries. We then extract the pages whose length is 30% or more shorter than our representative length for that domain. We find 24,381 samples are outliers, or 5.1% of our initial set.

5.3.1.3 Clustering & Identifying Page Signatures

After extracting the set of potential block pages, we cluster the HTML documents using single-link hierarchical clustering, which does not require that we know the number of clusters beforehand. We use term frequency-inverse document frequency with 1- and 2-grams to generate feature vectors using scikit-learn, a machine learning library in Python [300]. This resulted in 119 clusters, which we examined by hand and used to extract all pages that were potential signals of geoblocking. The CDNs that we identified were Akamai, Cloudflare, Amazon CloudFront, SOASTA, Incapsula, and Baidu. We also identified Google AppEngine, a hosting service, serving block pages. Our clustering method also identified three CAPTCHA services, namely Cloudflare, Baidu, and Distil Networks. We also identified the Cloudflare JavaScript challenge page. We chose also to include a fingerprint for the nginx `403 Forbidden` page and the Varnish `403 Forbidden` page. Finally, a large cluster represented Airbnb, which states on its block page that it does not serve its website to users in Crimea, Iran, Syria, and North Korea. As an obvious example of geoblocking, we included this block page to see whether their stated blocking practices aligned with what we observed.

We identify 5 pages that are explicitly geoblocking: Cloudflare, Amazon Cloudfront, Baidu, Google AppEngine, and Airbnb.

5.3.1.4 Resampling Block Pages

Finally, we identify all instances of the above block pages in our entire dataset. We took the country-domain pairs where we saw at least one instance of an explicit block page and sampled them 100 additional times, in order to explore how consistently we observe the geoblock page with different size samples. From the population of 100 measurements per country-domain, we take 500 samples of each size and find how many returned the block page. The results of this experiment can be seen in Figure 5.1.

Therefore, in every country in which we observe any of our block pages, we sample that

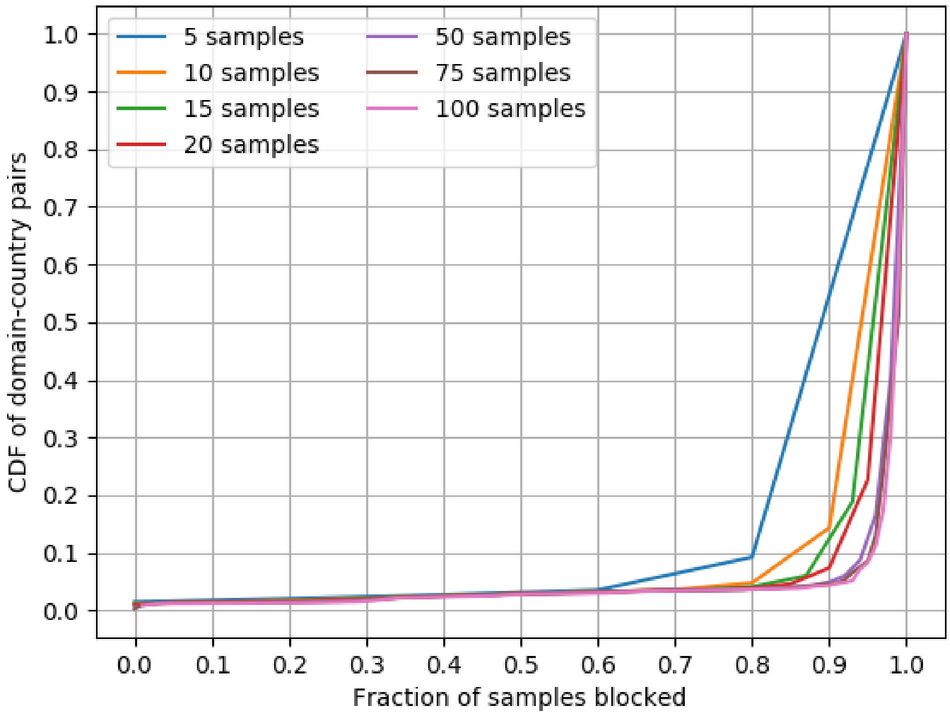

Figure 5.1: Consistency for various sample rates. This CDF shows the consistency of geoblocking for different sample rates for domain-country pairs where we expect to see a geoblock page. (see Section 5.3.2). A sample size of 20, which we use to confirm geoblocking, yielded only 3.9% of domain-country pairs with less than an 80% geoblocking rate.

domain 20 times in order to gain a higher confidence that the signal was correct. We then set a threshold of 80% agreement for the domains we consider geoblocked.

5.3.1.5 Evaluating Metrics

After conducting measurements, we evaluate some of the heuristics we chose.

Page Length Heuristic After extracting a set of 14 block pages from our clusters (see Section 5.3.1.3), we returned to this metric to evaluate its effectiveness. We found that the overall recall was only 58.3%. This metric was far more accurate for some block pages than others; the relative recalls are listed in Table 5.2. We also examine the difference in

Table 5.2: Recall for block pages and other content for Top 10K sites. Here are our recall rates for the 30% difference in length metric.

	Recalled	Actual	Recall
Akamai	1446	3313	43.7%
Cloudflare	406	433	93.8%
AppEngine	381	499	76.4%
Cloudflare Captcha	1181	1264	93.4%
Cloudflare JavaScript	664	1001	66.3%
Amazon CloudFront	36	95	37.9%
Baidu Captcha	128	139	92.1%
Baidu	3	3	100.0%
Incapsula	362	710	51.0%
Soasta	36	36	100.0%
Airbnb	49	49	100.0%
Distil Captcha	315	1028	30.6%
nginx	1524	2656	57.4%
Varnish	22	22	100.0%
Total	6553	11248	58.3%

size between each sample and the length we had compared it against to find the difference, as shown in Figure 5.2. This shows that selection of length cutoff is relatively arbitrary between 5% and 50%—both will yield around 20% false negative across the whole dataset.

We chose percentages of page length following the methodology of Jones, but we note that other experimentation showed that using raw length differences is not as effective. Using percentages normalizes the lengths of pages, while raw length differences excessively penalize long pages. The purpose of this metric is as a rough heuristic, so while it is fortunate it is effective, it is not critical that it be extremely discerning.

Initial Sample Size With the dataset in hand, we look at the probability of seeing a block page with only three initial samples per country. To do this, we take the set of explicit geoblocking domain and country pairs in order to measure how likely it is that we would *not* see the block page with different sample sizes. Because we expect the block page to be served every time, we are measuring the rate of other failures, for example proxy errors, transient network failures, and local filtering like a corporate firewall.

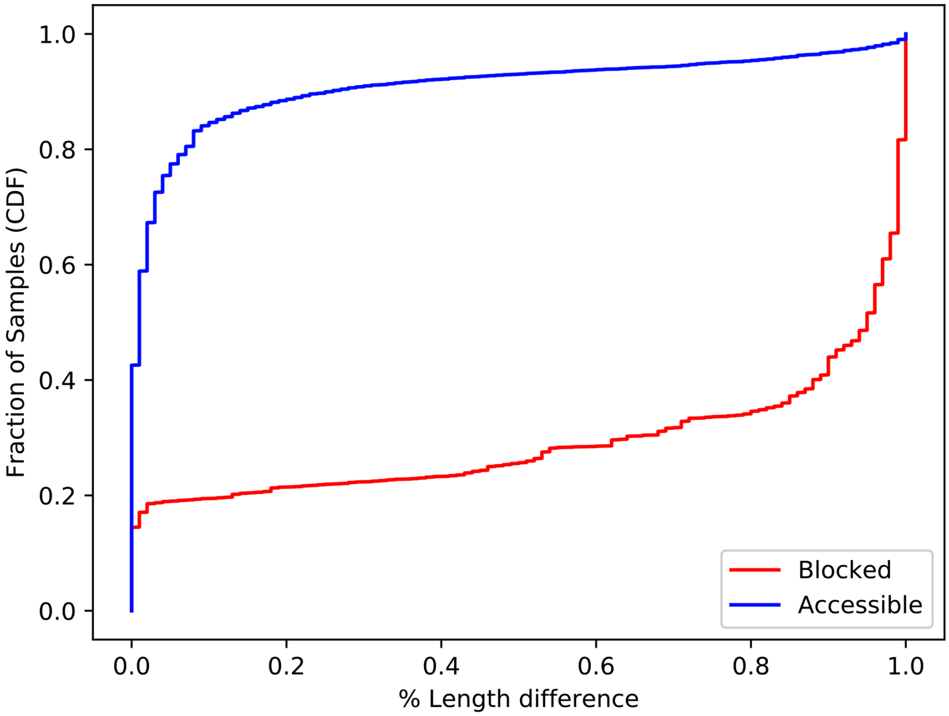

Figure 5.2: Relative sizes of block pages and representative pages. After selecting the longest observed instance of each domain across the top 20 geoblocking countries, we compare this page length with each sample and plot the length difference. The blocked pages are the samples that match one of our block page fingerprints.

We sampled each of these domain-country pairs 100 times. From each set of samples, we then selected 500 random combinations of different sample sizes to detect how many combinations would not yield a block page. For a sample size of 3, only 1.7% of our country-domain pairs did not yield at least one block page. The relationship between sample rate and false negatives can be seen in Figure 5.3.

5.3.2 Results

Overall we observe 596 instances of geoblocking by 100 unique domains in 165 countries. We were served explicit geoblock pages from Cloudflare, Baidu, Amazon Cloud Front, Google App Engine, and Airbnb. We also detected several other kinds of content, including Captchas and nginx error pages, but we restrict our analysis only to pages that

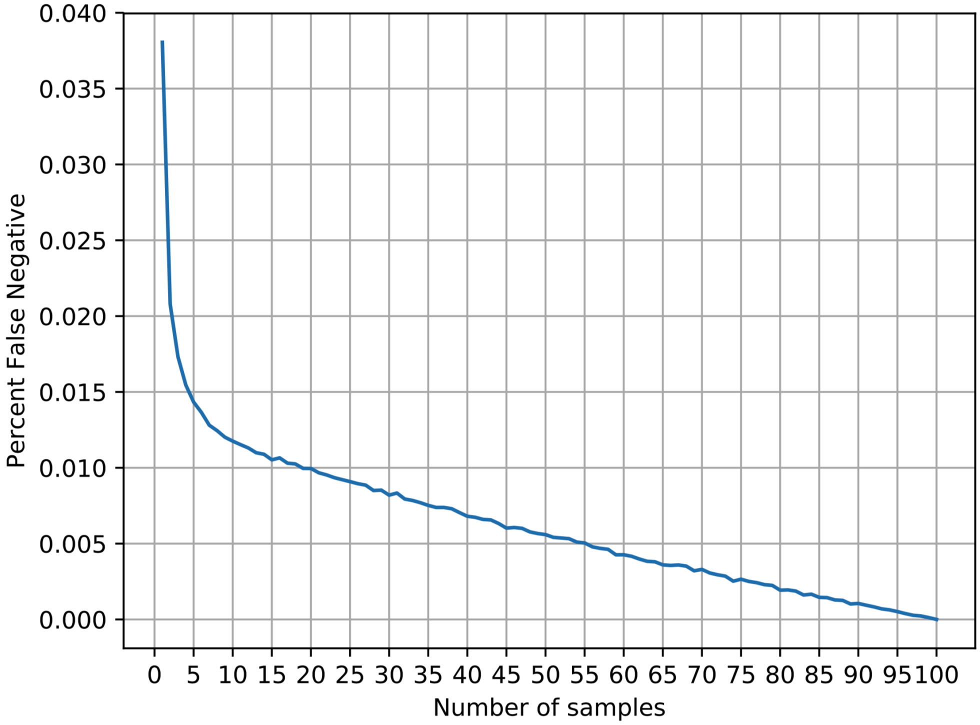

Figure 5.3: False negative rate for known geoblockers. This graph shows the rate of false negatives, where we see no instance of the block page, for different sampling rates of known geoblocking domain and country pairs.

explicitly signal that they are blocking due to geolocation.

Even for the domains that explicitly signal geoblocking, we do not observe the block page in 100% of samples in a country for just under half of all domain-country pairs. Some of these discrepancies can possibly be attributed to local connection interference, which might be observed if the Luminati device is inside of a corporate firewall. One domain, `http://makro.co.za`, returned a block page for each of our 3 initial measurements in 33 countries, but did not display any geoblocking when we sampled that domain again 20 times in each country several days later, suggesting that we may have observed a change in policy away from geoblocking. Other, smaller discrepancies may yet be attributed to geolocational errors. We limit our analysis to those country-domain pairs that yield a block page at in least 80% of the total 23 samples, which eliminates 77 instances, or 11.4%, in order to account

Table 5.3: Most geoblocked categories by CDN. We show the top 10 cateogories of the geoblocked domains by CDN.

	Cloudflare	AppEngine	CloudFront	Total
Shopping	18	10	0	28
Business	9	3	1	13
Techonology	0	9	0	9
News/Media	3	6	0	9
Advertising	1	7	0	8
Job Search	4	0	0	4
Newsgroups	0	4	0	4
Sports	1	2	0	3
Education	1	1	0	2
Entertainment	1	1	0	2
Other	5	1	4	10
Total	43	44	5	92

for some of these transient errors. The distribution of the sample agreement is shown in Figure 5.4.

Table 5.4 displays the categories in which we saw geoblocking. Shopping, Travel, and Business all appear at the top of the list, indicating that consumer market segmentation may be a common motivation for geoblocking. We also see many other categories which are more prevalent in blocking, including Advertising and Job Search. Child Education tops the list in terms of fraction of category blocked, but this is a small category of sites that we tested, and only one geoblocks (`pbskids.com`, which as a U.S. site possibly blocks due to federal sanctions).

Table 5.5 shows the TLDs which geoblock the most. Sites using `.com` geoblock the most by a wide margin, which is likely just a simple reflection of the prevalence of `.com` sites in the Top 10K. Notably, outside of `.net` and `.org`, all other TLDs were country based. Although there were multiple sites with country TLDs that practiced geoblocking, this does not appear to be a major indication of policy within the Top 10K sites.

The most commonly geoblocked countries are also shown in Table 5.5. The top four countries are Syria, Iran, Sudan, and Cuba, by a wide margin. These are notably all

Table 5.4: Geoblocked sites by category. We show the 20 categories of tested sites in the Alexa 10k Luminati data. "Geoblocked" is the number of unique sites we observed being blocked in at least one country.

Category	Tested	Geoblocked
Child Education	8	1 (12.5%)
Advertising	120	8 (6.7%)
Job Search	97	4 (4.1%)
Shopping	787	29 (3.7%)
Travel	168	6 (3.6%)
Newsgroups and Message Boards	143	4 (2.8%)
Web Hosting	41	1 (2.4%)
Business	758	13 (1.7%)
Sports	179	3 (1.7%)
Personal Vehicles	78	1 (1.3%)
Reference	176	2 (1.1%)
Health and Wellness	92	1 (1.1%)
News and Media	938	9 (1.0%)
Freeware and Software Downloads	115	1 (0.9%)
Information Technology	1,239	9 (0.7%)
Games	348	2 (0.6%)
Entertainment	442	2 (0.5%)
Finance and Banking	454	2 (0.4%)
Education	583	2 (0.3%)
Total	6,766	100 (1.6%)

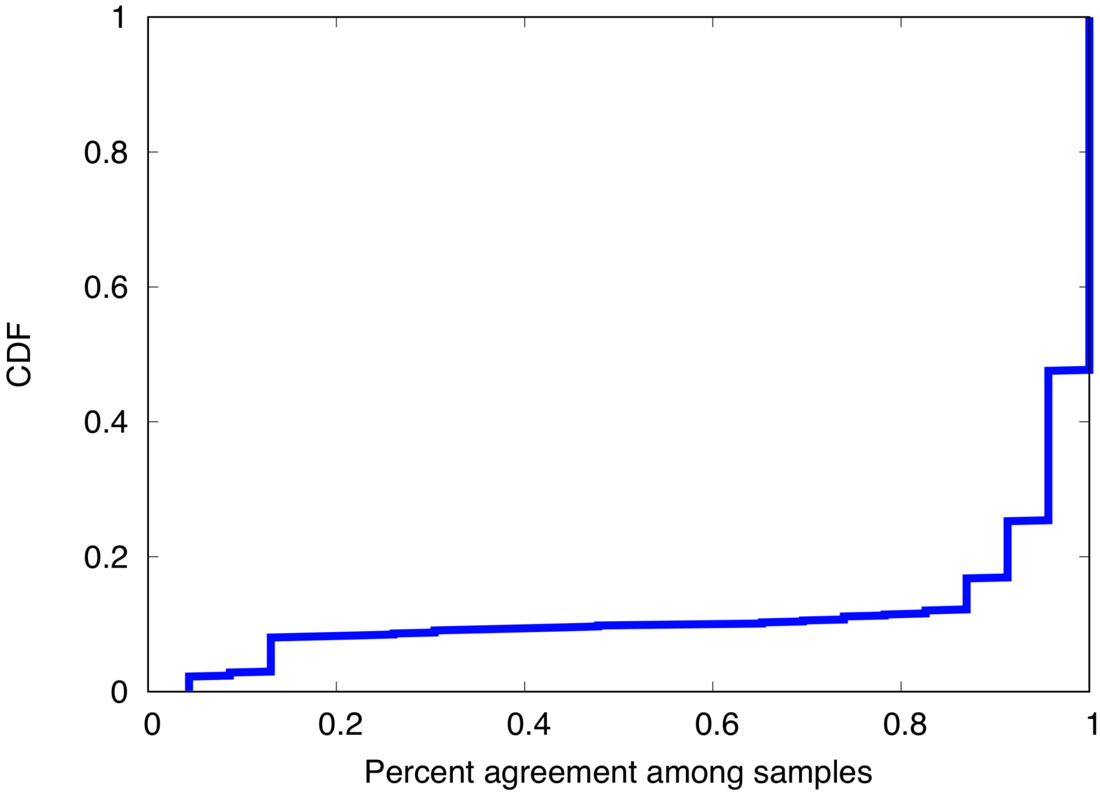

Figure 5.4: Consistency of geoblocking observations. The CDF of the number of probes of a given site before seeing a non-geoblock page. For the vast majority of sites seen geoblocking, the block page was seen in >80% of probes.

countries sanctioned by the United States. Nigeria, China, and Russia are also more commonly geoblocked as compared to other countries.

5.3.2.1 Geoblocking by CDNs

The largest set of geoblocking websites are served by content distribution networks, three of which meet our criteria as explicit geoblockers: Cloudflare, Google AppEngine, and Amazon CloudFront. Table 5.3 shows the categories of geoblocking sites on each CDN. Shopping is the most prevalent on Cloudflare and AppEngine, but AppEngine hosts more geoblocking Information Technology, News, Advertising, and Message Board sites than Cloudflare. We see only one site on CloudFront from the top categories, with the others being dispersed through less common categories.

Table 5.5: Top TLDs and geoblocked countries for Top 10K sites where we detected geoblocking.

TLD	Count
.com	70
.net	3
.org	3
.fr	2
.it	2
.jp	2
.in	2
.au	1
.br	1
.sg	1
Other	13
Total	100

Country	Count
Syria	71
Iran	67
Sudan	66
Cuba	66
China	11
Nigeria	11
Russia	10
Brazil	8
Iraq	6
Pakistan	5
Others	275
Total	596

Table 5.6: Geoblocking among Top 10K sites, by country. These countries experienced the most geoblocking.

	Cloudflare	CloudFront	AppEngine	Total
Syria	20	3	44	71
Iran	20	3	37	67
Sudan	20	2	44	66
Cuba	20	2	44	66
China	8	2	0	11
Nigeria	10	1	0	11
Russia	7	3	0	10
Brazil	8	0	0	8
Iraq	5	1	0	6
Pakistan	3	2	0	5
Other	127	148	0	275
Total	248	167	169	596

Table 5.6 shows the breakdown of countries blocked by each CDN. Google AppEngine explicitly blocks Cuba, Iran, Syria, Sudan, Crimea, and North Korea due to sanctions [166], and we can observe the effects of this. We do not see AppEngine blocking in any other country. We see a similar increase in geoblocking for these countries in Cloudflare and CloudFront's sites, but AppEngine sites block these countries at a much higher rate than the other two. Geoblocking from Cloudflare sites is overall much more visible than the from the other two CDNs.

We use the methods described in Section 5.4.1 to obtain the number of sites in the Alexa Top 10K using each of these CDNs or hosting providers. We find 1,394 Cloudflare fronted domains, 364 Cloudfront domains, and 108 Google AppEngine domains. Google AppEngine has by far the highest rate of geoblocking, with 40.7% of its customers inaccessible in at least one country. Comparatively, only 3.1% of Cloudflare customers geoblock, and only 1.4% of Amazon Cloudfront customers geoblock in at least one country.

5.3.2.2 Other observations

While in general we observe geoblocking to be a country-wide phenomenon, we have observed a counterexample to this. The website geniusdisplay.com served an nginx block page for most of our measurements in Russia, but we received some AppEngine block pages for it (few enough that it did not meet our threshold value for considering the site geoblocked). Upon manual inspection, we noticed that we only received the AppEngine page when attempting to access the site from IPs in Crimea, suggesting that at least Google AppEngine is displaying geoblocking at a finer granularity than country-wide.

We observed two other explicit geoblocking pages that we do not include above. We observed one website (`fasttech.com`) in China that served a Baidu blockpage, which is nearly identical Cloudflare blockpage in content. We also observed 347 instances of geoblocking from Airbnb on various geographic TLDs, exclusively blocking Iran and Syria.

In addition to explicit geoblock pages, we also observed several other block pages that were either not geoblocking but may contribute to the overall discrimination against certain countries, e.g. captchas, or ambiguous pages for which we cannot confidently say whether blocking is based on geolocation. This set of 200,417 observations includes captchas from Cloudflare, Baidu, Distil, a JavaScript challenge page from Cloudflare, and ambiguous block pages from SOASTA, Akamai, and Incapsula.

5.4 Alexa Top 1m

In this section we expand our results from Section 5.3 to look at the prevalence of geoblocking of five services in the Alexa Top 1M: the CDNs Cloudflare, Amazon Cloudfront, Akamai, Incapsula, and the hosting provider Google AppEngine.

5.4.1 Methods

5.4.1.1 Identifying CDN Population

In order to find the rate of geoblocking in the Top 1M by CDN or hosting provider that we identified in the previous section, we first needed to find the population of domains using each service from which we could sample.

Several CDNs were simple to identify; when requesting a site fronted by Cloudflare, Amazon Cloudfront, and Incapsula, a special header is appended to the response: `CF-RAY`, `X-Amz-Cf-Id`, and `X-Iinfo`, respectively. We used ZGrab to request all domains in the Top 1M and identified all domains that returned these headers anywhere in the redirect chain. With this method, we found 109,801 Cloudflare, 10,856 Amazon Cloudfront, and 5,570 Incapsula domains in the Alexa Top 1M.

To identify Akamai domains, we send a Pragma header [13] to all domains in the Alexa Top 1M, which triggers the Akamai edge server to insert cache-related headers into the response. If we saw these Akamai cache headers anywhere in the redirect response chain, we considered the domain to be fronted by Akamai, because at some point during the request there would be an opportunity for Akamai to block the request. We discovered 10,727 Akamai domains in the Top 1M.

Finally, we consider Google AppEngine. According to Google forums [167], Google AppEngine traffic will stem from IPs that are discoverable by doing a recursive lookup on `_cloud-netblocks.googleusercontent.com`. Using this method, we found 65 IP blocks and 16,455 domains in the Top 1M hosted on AppEngine.

In total, we found 152,001 unique domains in the Alexa Top 1M that use one of these services. 1,408 domains showed signs of using two services. For example, `zales.com` contained both the Incapsula and Akamai headers. Because these domains have the potential to be blocked by either service, we consider them to be customers of both.

5.4.1.2 Sampling

We categorized these domains using FortiGuard. We then excluded the same risky categories as before: categories relating to pornography, violence, drugs, malware, dating, censorship circumvention, and meaningless or unknown categories. We also eliminated any domains found in the Citizen Lab Block List. This left us with 123,614 domains. Finally, we took a 5% random sample of these domains to create a test list of 6,180 domains.

Using the same method as in Section 5.3.1, we first sample each domain 3 times in each country. For our explicit geoblockers (Cloudflare, Amazon Cloudfront, and Google AppEngine), for each country-domain pair where we see at least one block page, we sample again 20 times. For our non-explicit geoblockers (Akamai and Incapsula), for every domain where we see a block page in any country, we sample the domain again 20 times in every country.

5.4.1.3 Dataset

Of the 6,180 domains we sampled, 26 never successfully responded to our requests. We saw 3 domains indicating that Luminati would not complete the request via the

Table 5.7: Geoblocking among Top 1M sites, by country. These countries experienced the most geoblocking.

	Cloudflare	CloudFront	AppEngine	Total
Iran	64	7	107	178
Sudan	55	2	112	169
Syria	55	3	110	168
Cuba	50	3	112	165
China	24	10	0	34
Russia	18	10	0	28
Ukraine	18	4	0	22
Nigeria	12	5	0	17
Brazil	12	5	0	17
Romania	13	3	0	16
Other	527	224	0	751
Total	848	276	441	1,565

`X-Luminati-Error` header. This is only 0.05% of our sample, compared to 0.2% of Alexa Top 10K domains, indicating that more popular websites are more protected by Luminati. Furthermore, 90% of the domains we investigate saw an error rate of 3.0% or less, where error here indicates that we were unable to get a response from the site, either due to proxy errors or errors such as timeouts and lengthy redirect chains. This is markedly lower than our Alexa Top 10K study.

5.4.2 Results

We find that geoblocking in the Alexa Top 1M follows similar patterns to those in the Alexa Top 10K, as we will report in this section.

5.4.2.1 Explicit Geoblockers

Looking first at the providers that explicitly geoblock (specifically Cloudflare, Amazon Cloudfront, and Google AppEngine), we see 1,565 instance of geoblocking across 176 countries—all countries except Seychelles. This accounts for 238 unique domains in 176 countries. The most geoblocked countries are shown in Table 5.7. The median number of sites blocked in each country is 4, indicating that most countries have at least a few domains preventing access by their residents.

In the Alexa Top 1M, AppEngine remains the provider with the most geoblocked domains; of the 667 Google AppEngine domains in our 5% sample of Top 1M CDN sites, 112 domains displayed the geoblock page, or 16.8%. All but 5 domains were blocked in each of Syria, Sudan, Iran, and Cuba; 5 domains were censored in Iran, preventing us from measuring geoblocking, and 2 were censored in Syria. This is much lower than the rate of 40.7% of AppEngine domains in the Top 10K that showed signs of geoblocking. Amazon Cloudfront had 16 of its 512 domains practicing geoblocking, a rate of 3.1%, which is slightly higher than we observed in the Top 10K. Finally, Cloudflare saw geoblocking on 110 of 4,283 Cloudflare domains at a rate of 2.6%, which is comparable to what we observed in the previous study.

As can be seen in Table 5.7, Iran, Syria, Sudan, and Cuba are the countries experiencing the most geoblocking in this dataset by raw number of inaccessible domains. We also see other large countries such as Russia and China appearing in the top ten.

We can also see that Google AppEngine only geoblocks in Iran, Syria, Sudan, and Cuba, which is consistent with the list of countries Google claims to block. North Korea had no Luminati hosts for us to probe from, and we may miss Crimea due to exploring geoblocking at a country granularity rather than regionally. This is one way in which our study may be expanded.

The distribution of domains that geoblock in at least one country across categories can be seen in Table 5.8. By raw numbers, Shopping is still the most geoblocked category, followed by Business, Information Technology, Personal Vehicles, and News and Media. By ratio of tested domains in each category, Personal Vehicles and Shopping each show that at least 10% of domains in that category practice geoblocking in at least one country, along with Auctions, which is not in the top 15. This is a significant number of domains in each of these categories that are potentially inaccessible to users.

Table 5.8: Geoblocked sites by top category. We show the top 15 of 25 geoblocked categories of *explicit* geoblocking sites by number of domains in the Alexa 1M Luminati data. "Geoblocked" is the number of unique sites we observed being blocked in at least one country.

Category	Tested	Geoblocked
Shopping	418	59 (14.1%)
Business	1,176	51 (4.3%)
Information Technology	1,016	34 (3.3%)
Personal Vehicles	79	16 (20.3%)
News and Media	345	12 (3.5%)
Society and Lifestyle	148	7 (4.7%)
Health and Wellness	146	5 (3.4%)
Travel	153	5 (3.3%)
Personal Websites and Blogs	176	4 (2.3%)
Education	239	4 (1.7%)
Games	206	4 (1.9%)
Sports	121	4 (3.3%)
Reference	81	4 (4.9%)
Job Search	42	4 (9.5%)
Finance and Banking	108	4 (3.7%)
Other	1,008	21 (2.1%)
Total	5,462	238 (4.4%)

5.4.2.2 Non-Explicit Geoblockers

Akamai and Incapsula are also CDNs that offer their customers the opportunity to geoblock. However, both services display the same block page for other errors, making it more difficult to distinguish geoblocking from bot detection or other server errors. Because we do not have multiple hosts in each country with which we can manually check whether a domain is blocked, it is not possible for us to say with complete confidence which domains are geoblocking. However, here we can reason about what metrics possibly indicate geoblocking for these CDNs.

Intuitively, we are looking for domains that consistently send a block page in some countries and consistently do not in others. One metric we look at here is thus the consistency of block page within country. For all domains where we see an Akamai or an Incapsula block page, we consider any country receiving the block page at least 80% of the time to be consistent; each domain then has an overall consistency score that is the percent of countries that are consistent for each domain. For some domain where only two countries are blocked 100% of the time and the rest of the countries never see a block page, this would be a consistency score of 100%. Alternatively, if a domain had three countries each seeing 90% of samples returning a block page and one domain with 20% block pages, it would have a consistency score of 75%.

Applying this metric to our explicit geoblockers, we see that they each only have a consistency rate of 100% about 85% of the time. For Akamai and Incapsula, the rate is much lower; they have a 100% consistency rate only 13.9% and 15.9%, respectively. This is a good verification that Akamai and Incapsula are noisy block pages. Therefore, in order to be conservative, we will discuss only those domains that do not show a block page in all countries and that have 100% consistency.

We find 201 instances of geoblocking with Akamai and 200 instances with Incapsula. This encompasses only 14 of 101 domains that returned the block page at least once for Akamai and 17 of 107 domains for Incapsula. Both sets of domains see China, Russia, Cuba, Iran, Syria, and Sudan as the most blocked countries, indicating that we are indeed isolating geoblocking in these domains, if not exhaustively across all Akamai and Incapsula domains.

5.5 Cloudflare Validation

Cloudflare provided us with data that confirmed our measurements and gave further insight into the practice of geoblocking.

Cloudflare offers customers the ability to set specific access rules for their domains via the Firewall Access Rules feature [93]. These rules allow customers to whitelist, challenge, or block visitors based on IP address, country, or AS number. These rules give the site owner more fine-grained control over the visitors that Cloudflare allows to access their site. For instance, a website that is under attack might enable rules to present CAPTCHAs to visitors to cut down on bot traffic, or a retail site that only ships to certain countries may wish to block visitors based on geolocation.

The ability to block visitors by country is reserved for Cloudflare's Enterprise customers. Free-, Pro-, and Business-level customers still have the ability to present challenges by countries, but a human visitor from those countries could still access the site by completing a challenge. However, due to a regression, the country-blocking feature was enabled for customers of all tiers from April to August 2018. Cloudflare was able to provide us with a July 2018 snapshot of all active country-scoped rules set by their customers, which falls during the regression period. Each rule in the dataset includes the rule action (block, whitelist, challenge, js_challenge), the target country, the number of affected zones, the zone customer tier, and the rule activation date. Cloudflare zones are roughly defined as a domain and all its subdomains. We publish aggregates of the data to avoid revealing any individual customer information.

The data displayed in Table 5.9 shows that the scale of geoblocking we observed for Cloudflare was roughly accurate. Because North Korea had no Luminati vantage points,

Table 5.9: Most geoblocked countries by Cloudflare customers, by account type. These countries experienced the highest rates of geoblocking by Cloudflare customers. “Baseline” gives the percentage of zones for each account type that have geoblocking enabled against any country.

Country	All	Enterprise	Business	Pro	Free
Baseline	1.93%	37.07%	2.69%	2.56%	1.72%
Russia	0.22%	4.90%	1.14%	0.44%	0.19%
China	0.22%	3.11%	1.16%	0.46%	0.20%
North Korea	0.20%	16.50%	0.38%	0.17%	0.10%
Iran	0.18%	15.57%	0.39%	0.13%	0.09%
Ukraine	0.18%	3.89%	0.71%	0.38%	0.15%
Romania	0.14%	3.63%	0.49%	0.24%	0.12%
India	0.14%	4.18%	0.48%	0.23%	0.11%
Brazil	0.13%	3.87%	0.43%	0.16%	0.11%
Vietnam	0.13%	3.08%	0.33%	0.16%	0.11%
Czech Rep.	0.11%	3.66%	0.40%	0.15%	0.09%
Indonesia	0.11%	2.24%	0.39%	0.12%	0.10%
Iraq	0.10%	3.99%	0.32%	0.09%	0.08%
Croatia	0.10%	3.44%	0.24%	0.13%	0.08%
Syria	0.10%	13.74%	0.17%	0.06%	0.02%
Estonia	0.10%	3.28%	0.32%	0.14%	0.08%
Sudan	0.10%	13.57%	0.12%	0.04%	0.02%

we were unable to measure how extensively it was blocked. This is one observation we gain from the Cloudflare data that was not visible in our measurements: North Korea is the third most geoblocked country, and the most blocked country of enterprise customers. This is particularly telling of the motivations of companies to geoblock. North Korea is under U.S. sanctions, but likely poses little to no other risk to companies because of the country's relatively low access to the Internet and virtual absence from international commerce, indicating that compliance with sanctions alone is a primary driving force of geoblocking for larger customers.

As the customers of Cloudflare with Business, Pro, and Free accounts were unable to use geoblocking features until April 2018, we can see in Table 5.9 that a significant number of accounts activated geoblocking in the last 3 months, especially considering that there are far more domains on Business, Pro, and Free accounts than for Enterprise accounts. This suggests that where the functionality is available, many websites will opt to use the feature. Additionally, we see that the free tier customers block China and Russia at a higher rate than other countries, including countries under sanctions, suggesting that the motivation for blocking these sets of countries might be different for sites without an enterprise-level contract with Cloudflare. Notably, Iran and North Korea experience significantly lower rates of geoblocking relative to other geoblocked countries for business, pro, and free accounts.

In Figure 5.5, we see the accumulation of blocking rules over time. Notably, North Korea, Iran, Syria, Sudan, and Cuba follow the same pattern, indicating that customers who activate blocking rules tend to treat these countries similarly—although notably not exactly the same, as Iran and North Korea experience more geoblocking than the other three.

5.6 Discussion

In this section, we will discuss the insights we gained from this study and the remaining challenges and opportunities in studying geoblocking.

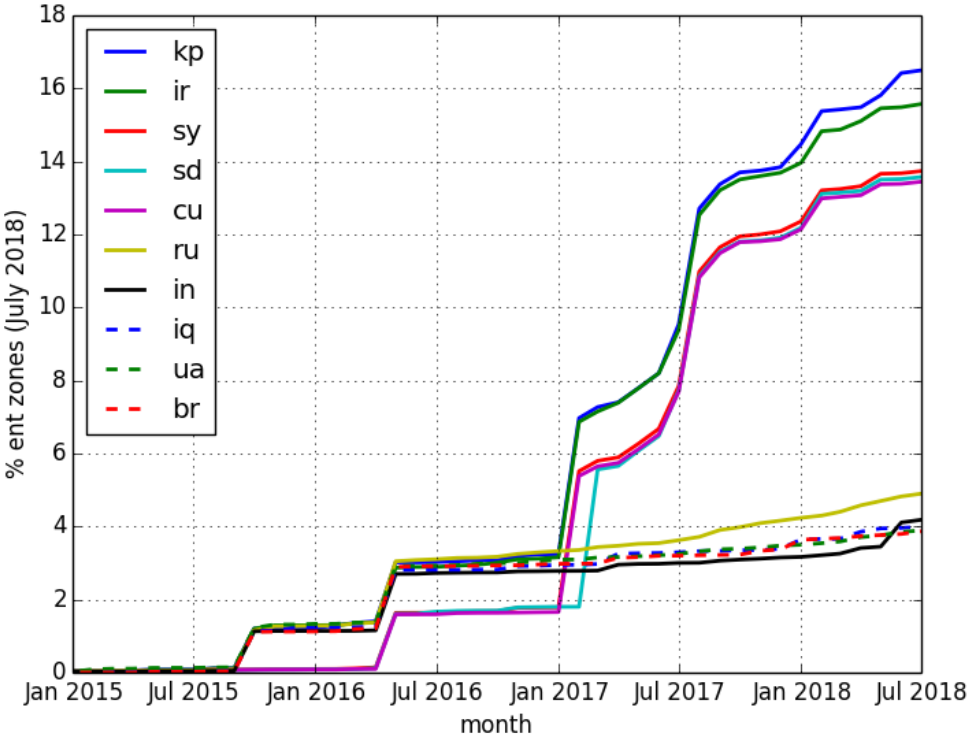

Figure 5.5: Cloudflare Enterprise customers' activation of geoblocking over time, by geoblocked country. This graph shows the activation dates of blocking rules over time for the Enterprise customers (ent) who had country-scoped geoblocking rules active in July 2018.

5.6.1 Geoblocking and Censorship

We want to consider how censorship and geoblocking may be related. First, we consider how censorship measurement may have been impacted by the presence of geoblocking. Beyond our active measurements, we looked for evidence of the block pages we identified appearing in censorship measurement datasets. We turn to the existing OONI measurement corpus [143]. OONI measurements are user submitted reports from around the world, created with a provided software client. The software draws URLs to test from the Citizen Lab list [88], a widely used list of censored domains, and records the full body and headers of the response. All together, domains have been tested 87 million times by OONI clients.

We find 8,313 cases in 139 countries where OONI responses match the explicit signals of geoblocking we describe in Section 5.3. Instances occur in all of the 12 countries where OONI identifies state censorship. More importantly, these cases occur at least once for 97 domains, or 9%, of the global test list, indicating that geoblocking could be a significant confounding factor in censorship measurement.

This is also only a conservative estimate of how often server blocking is experienced in OONI measurements. The OONI methodology compares client measurements against a control, but that control is often made over Tor, which is also subject to blocking [340]. Saved reports only include the status and headers of the control measurement that is used for comparison, and not the actual contents of that request. As such, it is difficult for us to retroactively understand if a request is made at a time when a site was truly unavailable, or whether the control measurement was also blocked. This is a sizable effect. For example, there were 36,028 OONI measurements to sites using Akamai and Cloudflare infrastructure where the control measurement returned a `403` status code, compared to 14,380 requests where the local measurement was blocked but the control succeeded. The majority of these block pages in the OONI database, more than 30,000 in all, are correlated to blocking of the control request rather than the in-country probe data.

Conversely, it is certainly possible that censorship may disguise itself as geoblocking. A censor could inject or redirect to a mimicked geoblock page as a way to censor content without taking responsibility. To our knowledge, we did not observe any instances of this. Furthermore, we believe the incentive for companies to enable full-page geoblocking to be misaligned with traditional censorship, in which a government dictates what content should not be available to its own constituents. If a government were to demand a website enable geoblocking for its own IP space, the website would have little reason to comply. Large companies with multiple domains may need to cooperate with a censorious country, but we have seen in practice that this cooperation more frequently appears as selective access and content filtering rather than full denial of access [274, 132].

5.6.2 CDNs Enable Geographic Discrimination

Content Distribution Networks offer a valuable service for websites by decreasing latency to their users worldwide while providing a baseline level of security and protection that is otherwise nearly impossible to implement at the hosting server. With increase in value added by CDNs coupled with falling costs (Cloudflare, for example, offers basic services for free), more websites are opting into the service. While this makes security features accessible to far more website than previously, this trend increases centralization and enables more sites to use CDNs to control what content is served to which users on the Internet. CDNs are also incentivized to implement tools that add value to their big ticket customers, and they may choose to expose this functionality to most or all of their other users. This gives even the smallest websites the ability to enact fine-grained control over the ways in which their content is served, and to whom.

This is exactly what occurred with Cloudflare between April and August 2018. The ability for Business, Pro, and Free customers to use the geoblocking feature was enabled for 4 months, where it had previously only been available to Enterprise customers. By July 2018, when Cloudflare provided us a snapshot of data about blocking rules, customers in different tiers had already extensively utilized the geoblock feature. Although Cloudflare reverted to its former access model, in which only Enterprise customers could geoblock, we were provided with a valuable insight into what unrestricted geoblocking might look like. In the end, website operators seem to be fairly liberal in activating features that harshly restrict access to content. Customer access to these tools should be limited.

5.6.3 Limitations & Future Work

Positive identification of geographic blocking provides an exciting first step in studying this phenomenon, but also opens many more doors for future work. While we believe that this approach gives us insight into the most extreme form of geoblocking, namely the total denial of access, our method may miss custom geoblock pages that are not significantly different from the typical page. We also observed consistent timeouts for certain websites in only some countries; an exploration of whether timeouts are another method of geoblocking would be useful, although much more difficult to differentiate from censorship. Additionally, for instances in which a block page is also used for other access control like bot detection, our technique does not provide access to verify our observation through an interactive browser.

In this vein, additional work could be done to simulate a real browser in the automated requests from VPSes. As mentioned in Section 5.2, early experiments show that adding a full set of headers on ZGrab can reduce the rate of false positives significantly. While this does not eliminate the need for manual validation for non-explicit geoblockers, it does reduce the amount of manual work required to gain enough confidence in the data to automate the classification process.

Finally, discrimination that is not explicitly communicated to users is also important and much harder to measure. Prices are often different when a site is viewed from different locations, or some features may be removed. We do not capture these effects in our current blockpage-based discrimination measurements, and further work into automatically detecting geographic differences in functionality or access is vital to understanding geographic discrimination.

5.7 Related Work

The Internet is becoming increasingly regionalized due to sanctions, financial regulations, copyright and licensing rights, perceived abuse, or a perceived lack of customers. This issue is known to policy makers. The EU Parliament recently adopted a regulation to ban geoblocking for most types of online content to give users access to goods and services at the same terms, all over the EU [23]. The majority of the news has been either on geoblocking of multimedia products or geolocation-based price discrimination. We lack a global perspective on the extent of this phenomenon.

“Supply-side” censorship was noted as an important component of the censorship landscape in the initial announcement of the Open Net Initiative [290] but has remained relatively uncharacterized. Rather, the vast majority of studies focused on understanding and circumventing nation-state censorship, specifically in China [91, 397, 174], Iran [34], Pakistan [272, 220], and Syria [76]. These studies often illuminate a wide variety of censorship mechanisms such as country-wide Internet outages [110], the injection of fake DNS replies [30, 241], the blocking of TCP/IP connections [299], and HTTP-level blocking [111, 294, 211]. Relevant to our work, Jones et al. designed an automated way of detecting censorship block pages, which inform the user that an access to the web page is unsuccessful. Their fingerprinting technique uses page length and frequency vectors of words as features. In our study, we show that these features are not sufficient for detecting blocking by service providers.

This category of measurement studies, including ours, face a major hurdle: obtaining vantage points in target countries. There are research systems for this purpose, though they are often limited to network diagnostic tests. For example, RIPE Atlas has more than 10,000 vantage points but does not allow HTTP requests. ICLab provides 1,000 vantage points from popular VPN providers, but the VPN providers have their own customized policies and malicious marketing behaviors. A wide-ranging tool for censorship detection is provided by OONI [143]. OONI runs an ongoing set of censorship measurement tests from volunteer's devices and doesn't provide a platform for exploratory experiment design in order to mitigate risk to participants.

For gaining a representative residential platform, the Luminati platform has proven to be useful. The downside to Luminati is the cost of running measurements from their network. Chung et al. used Luminati to analyze End-to-End Violations in the Internet [87]. Huang used it to detect HTTP middleboxes [197].

Directly related to our work is a study by Khattak et al., which systematically enumerates and characterizes the blocking of Tor users by service providers [219]. The authors explored how much of the differential treatment received by users of the service was due to an explicit decision to block Tor versus the consequence of “fate sharing”—being blocked because of abuse. In work conducted concurrently with our study, Tschantz et al. explored the space of blocking and argued that different forms of blocking, including geoblocking, warrant more research [365]. Our study attempts to understand the role played by private companies in controlling access to different contents from different locations.

5.8 Conclusion

In this work we have presented the first wide-scale measurement study of the extent of website geoblocking. We found that geoblocking is occurring in a broad number of countries and that many CDN customers utilize the geoblocking services they provide. Furthermore, across the Alexa Top 10K websites, we are able to observe a wide variety of block pages using a semi-automated technique, which helped us discover new CDNs and services that enable geoblocking. We have further explored the extent to which this form of content discrimination can affect censorship measurement, and find that a significant portion of a major list of censored domains contains domains that we have observed to practice geoblocking. While geoblocking is a diverse phenomenon with many different instantiations, we believe that this first study has shown that the phenomenon is both significant, impacting many populations worldwide, and empirically tractable for further study.

CHAPTER VI

A Taxonomy of Privacy Risks & Harms[1]

Privacy is important for everyone, but not all people are equally burdened by the risks and consequences of privacy failures. For example, public disclosure of one's address may be uncomfortable for many people, but for a sex worker with an aggressive client, that disclosure could be dangerous or deadly. Of particular concern are members of "high-risk populations," or those with a heightened likelihood or heightened consequence of a privacy harm [341, 247], such as historically marginalized groups, those living with stigmatized health conditions, those who are targeted by governments or other persistent attackers, among others.

Through increased reporting on how privacy failures by major tech companies harm marginalized groups (e.g., sex workers [190], Native Americans [239], undocumented immigrants [155]), and through a burgeoning body of literature focusing on the needs and experiences of populations facing privacy harms (e.g., trans people [234], survivors of intimate partner violence [249], people with vision impairments [11]), we are reaching a critical mass of data looking at how privacy harms manifest, and how their impact differs across many different populations. By synthesizing existing work across disciplines and identifying common dimensions of risk, experienced privacy harms, and the digital mecha-

[1] This chapter is based on work that was led by Allison McDonald, in collaboration with Mohamed Abbadi, Yixin Zou, Tanisha Afnan, An Doan, Tamy Guberek, Kentaro Toyama, and Florian Schaub
Allison McDonald's time on this project was supported by a Facebook Fellowship and a Rackham Merit Fellowship.

nisms that enable or exacerbate these harms, we can observe patterns across populations that reveal broader implications for technology and policy. These insights will help researchers and practitioners minimize the likelihood of these harms. Furthermore, by identifying risks and harms across high-risk populations, we can demonstrate that many problems do not happen only at the margins, but affect a substantial number of people.

We present a framework of privacy harms that (1) taxonomizes common risk factors and privacy harms across high-risk populations; (2) identifies the mechanisms that can exacerbate or trigger risk factors such that they result in harm; (3) and demonstrates the connections between high-risk populations, risk factors, and mechanisms of harm.

While other work has taxonomized privacy harms (e.g., [344, 90, 293]), few have done so through the lens of individual and community risk. In an independent, parallel effort, Warford et al. [381] arrived at a similar set of risk factors to ours; however, our work goes further to taxonomize the *mechanisms* that lead risk factors to result in harm, and draw connections between risk factors, harms, and mechanisms. By grounding our understanding of privacy harms in the experiences of the most severely impacted groups, we not only provide insight on the facets of existing technology that create risk for particular people, but provide a tool for reasoning about systemic patterns that have a disparate impact on the privacy of marginalized and otherwise high-risk communities. Furthermore, through understanding and addressing the mechanisms that harm high-risk populations in particular, we stand to improve technology experiences for all users, across the risk spectrum.

Intended audience & use This framework provides a better understanding of the connections between privacy risks and harm, highlights gaps and opportunities in existing research for focusing on under-explored dimensions of risk, and demonstrates the need to center vulnerability and risk in privacy research [254]. By leveraging our framework, researchers should have a common language to reason about any high-risk population's privacy risks. This can help facilitate consistency in the privacy risks and technical problems that are investigated in future in-depth research with a population. Technology builders, maintainers, and policy-makers can use the taxonomy to review which of their mechanisms or policies may have an adverse impact on vulnerable populations.

We note that this framework intentionally focuses only on risks while eliding benefits. Many mechanisms will have both positive and negative impacts on communities, which practitioners and researchers will need to weigh in their work. We expect that the benefits of most mechanisms will be manifest, so this framework provides assistance in reasoning about the risks.

6.1 Related Work

Here we overview existing work on understanding risk for specific marginalized populations, as well as work theorizing and taxomizing privacy.

6.1.1 HCI Research on the Privacy of High-Risk Users

There is extensive work on understanding privacy harms and protective strategies for populations with heightened digital risk such as journalists (e.g., [257]), survivors of intimate partner violence (e.g., [249, 152]), children (e.g., [349, 226]), sex workers (e.g., [251, 346]), and many others. Our work supplements these in-depth studies by offering a cross-population meta-analysis of common risks.

6.1.2 The Role of Marginalization in Privacy Risks

For many high-risk populations, the source of safety risks stems from marginalization and stigmatization in society. Understanding how identities and experiences in the world shape one's experiences and risks online will help us more effectively contend with the root of the problem in considering technical solutions. Feminist legal scholarship in particular has a long history of grappling with the ways the law (fails to) account for the experiences of marginalized and otherwise oppressed people, and these insights can shed light on the way platforms and tech companies themselves may fall short in accounting for these same problems.

Central to understanding risk across many populations is the concept of *intersectionality*. Intersectionality is a term coined by the legal scholar Kimberlé Crenshaw, which describes how identities, such as race, class, and gender, intersect with one another to create unique experiences of oppression [103, 104]. Our taxonomy atomizes privacy risks and looks at trends *within* particular risk factors; however, in building new technologies and addressing existing harms perpetuated by technology, we should be careful not to overlook the unique ways many people are impacted when they hold a combination of risk factors and identities.

Relatedly, critical race theory addresses the relationship between race, racism, and power, and highlights how a race-neutral or colorblind approach to antiracism, which fails to account for the ordinary and entrenched nature of racism, ultimately serves the dominant group [114]. This naturally manifests in the technical systems we all operate with and within [286]. Of particular relevance, Ogbonnaya-Ogburu et al. [286] highlight in their paper on critical race theory for HCI that "interest convergence," or the tendency for power to be conceded only when it also serves the dominant group [114], is at play in much existing HCI research and technology development. This is a challenge research engaging with racial justice must contend with directly. Critical race theory also highlights the unique and essential perspective of voices of color in addressing race and racism [114]. Within computing research, this has been demonstrated through important autoethnographic work on experiences of race, racism, and power in computing (e.g., [286, 131]).

Scott Skinner-Thompson, in his book *Privacy at the Margins* [341], explicitly draws the connection between marginalization and a heightened need for privacy by highlighting that groups that are typically marginalized are both less likely to be protected by existing legal privacy protections and more likely to experience disproportionate harm from privacy violations. In this work, we further demonstrate the connection between risk factors, including and especially marginalization, and online privacy harms.

6.1.3 Research Theorizing Privacy

There are several existing taxonomies and theories of privacy that inform our approach to and understanding of privacy harms.

Solove's taxonomy of privacy is a useful starting point for understanding various types of privacy harms [344]. Solove notes that "privacy" is often used as a nebulous term and privacy harms are often difficult to demonstrate, making legal arguments about privacy violations challenging to build. In response, Solove proposes a focus on harms when a privacy violation occurs. He identifies four categories of privacy violations, each with a set of subcategories: (1) information collection, (2) information processing, (3) information dissemination, and (4) invasion.

While each of these privacy violations in and of themselves are problematic, the consequences of violations are often not immediately obvious, dispersed among many people, or manifest as an increased risk of some worse consequence. In following work, Citron and Solove articulate the cognizable privacy harms that can follow from privacy violations [90]. The authors identify fourteen different categories of harm, including physical, economic, reputational, chilling effects, discrimination, and autonomy harms, and discuss to what extent existing case law recognizes them. Both of these taxonomies are illuminating and are a valuable starting point for enumerating privacy harms. However, neither help us understand *who* is most likely to be impacted by these harms, nor the ways that companies and platforms can cause or enable the identified privacy violations.

Other frameworks and theories serve to help determine whether a particular platform or technology will create undue privacy harm, or be misaligned with people's privacy expectations and goals. Altman's privacy regulation theory [19] offers the critical insight that privacy regulation is not a fixed process; rather, individuals are constantly optimizing their privacy in various contexts through boundary regulation. Palen and Dourish adapted this theory to an online context and identified three boundaries [293]: (1) disclosure, in which individuals balance information publicity and privacy; (2) identity, in which individuals navigate self-representation and group inclusion/exclusion; and (3) temporality, in which individuals manage tensions between past, present, and future implications of their actions. Similarly, how the mechanisms that we identify manifest privacy harms depends on these three dimensions.

Nissenbaum's theory of contextual integrity [279] offers another way to reason about privacy violations through understanding informational norms, which vary based on the people and the context in which an exchange occurs. In short, a privacy violation occurs when information exchanges violate the norms of the situation: for example, it is appropriate that a patient shares personal medical information with their doctor; it is not appropriate for a doctor to share that personal medical information with other patients.

While contextual integrity can be a highly useful tool for estimating privacy violations, its reliance on norms to dictate what an appropriate information flow is may pose limitations. McDonald and Forte [254] highlight that, because norms are set by the dominant group in any given context, they may not reflect the interests or needs of marginalized people. For example, governments may require poor people to disclose a significant amount of information to obtain public benefits; while this has been normalized, it may undermine otherwise reasonable expectations of privacy by those participating [247]. McDonald and Forte join others (e.g., Pierce et al. [303]) in emphasizing that vulnerability should be central to our understanding of privacy.

Our taxonomy intentionally centers the privacy needs and experiences of high-risk populations. In doing so, we provide a taxonomy that helps not only to see how current technology is creating privacy harms for these communities, but also how certain needs are broadly not being met, and how particular risk factors are being transformed into harms. A recent framework from Warford et al. [381] follows this same pattern and surveys recent literature on "at-risk populations" to present a framework encompassing contextual risk factors and protective practices. Warford et al.'s risk factors are consistent with the factors we present here; because our taxonomy was developed independently before release of their paper, the consistency suggests that these risk factors are comprehensive and useful. The rest of our taxonomy diverges from Warford et al. by focusing on identifying privacy harms and the mechanisms that lead to them, rather than on protective behaviors.

6.2 Methods

To build a comprehensive taxonomy of privacy harms, we conducted an extensive literature search and review about different high-risk populations with a wide range of privacy risks. We aimed to sufficiently cover a broad set of risk factors and populations, in order to provide comprehensive insights about diverse categories of privacy harms. As this meta-analysis is qualitative and not intended to be exhaustive, we do not use the PRISMA statements for literature reviews [267, 292]; however, we do follow many of their reporting guidelines to increase transparency.

At a high level, our process was: (1) collect relevant literature; (2) read and summarize relevant data from the selected papers; (3) synthesize the data by population (including in-population contradictions); and (4) conduct cross-population thematic analysis.

6.2.1 Literature Search

We started our search by canvassing publications from a range of security, privacy, and HCI conferences and journals between 2016–2020: the ACM Conference On Computer-Supported Cooperative Work And Social Computing (CSCW), the ACM CHI Conference on Human Factors in Computing Systems (CHI), the Symposium on Usable Privacy and Security (SOUPS), the IEEE Symposium on Security & Privacy, the USENIX Security Symposium, and the Privacy-Enhancing Technologies Symposium (PETS). We expected these venues to be most likely to have research on the technical challenges of users. One author reviewed titles and abstracts to select papers that discuss the privacy, security, or safety needs of a high-risk population (i.e., any that faces a heightened risk or consequence of a privacy invasion) or a particular technical mechanism that is described or discussed with a focus on disparate impact among users/subjects. In total, we collected 133 academic studies for consideration.

As we reviewed papers, we expanded the set of relevant studies to include literature that was cited by or that cites our selected papers. This was to ensure that we include literature outside of computer science and HCI, as papers focused on a particular population typically also engage with relevant research from other domains like sociology, gender studies, history, etc., which can further contextualize privacy sensitivities of relevant populations.

We wanted to minimize the recreation of gaps that already exist in the privacy, security, and HCI literature. Thus, we also considered what populations are most likely to face heightened consequences of a privacy violation—for example, due to discrimination, limited resources, or high-risk jobs or circumstances—and conducted a broader search for relevant literature if certain populations had not come up in our previous search. To do this, we used keywords to search Google Scholar and news articles to find literature on the topic of privacy and safety for these populations.

Finally, we did not restrict literature collection to peer-reviewed work; where relevant, we reviewed additional sources of knowledge such as community-led reports (for example, *Posting into the Void* [50] from Hacking//Hustling, a sex worker tech collective) and investigative journalism around privacy risks (for example, "How ICE Picks Its Targets in the Surveillance Age" from the *New York Times* [155]).

6.2.2 Literature Review & Analysis

The seed set contained papers that were both highly relevant (e.g., papers specifically discussing the privacy risks of a population) and tangentially relevant (e.g., those that may touch on privacy concerns while investigating a separate topic). For each population, we started by reviewing the papers with the highest relevance, and added any relevant cited literature to the analysis. A population review proceeded until every paper was reviewed or until continued reviewing no longer yielded new information. In total, we reviewed

82 studies, reports, and articles involving the following populations: survivors of intimate partner abuse, Black people, Muslim women, older adults, children, people with stigmatized health conditions, people with impaired vision, LGBTQ+ people, sex workers, formerly or currently incarcerated people, migrants and refugees, activists, and journalists. An overview of populations and literature can be seen in Table 6.1.

For each paper, we completed a structured review that summarized the paper's method, findings, and limitations, as well as a distillation of the subject population's privacy-related risk factors (e.g., intimate partner abuse survivors have a persistent targeted attacker), the harms that result (e.g., anxiety, financial ruin), and the ways that harm was enabled (e.g., shared accounts, spyware). This review format was developed iteratively by having four researchers apply it to several papers from different populations. Authors then exchanged reviews and discussed how well the reviews extracted the relevant privacy risks, harms, and mechanisms while keeping important context and limitations from the original paper. Once the review format was finalized, five researchers contributed to reviewing and summarizing the literature.

When a reviewer had read several papers on a particular population, they summarized the findings for the population. These summaries served to synthesize risks, harms, and mechanisms from across papers, clarify whose perspectives may still be missing, and identify where and how the literature may disagree, including ways in which a population varies internally.

Finally, we conducted multiple rounds of analysis based on our structured paper reviews, while also frequently going back to source papers. Using affinity diagramming [196], we generated common themes between populations for risk and vulnerability, types and consequences of privacy harms, factors that led to privacy harms, types of sensitive information involved in privacy harms, and adversaries. Supplemented by affinity diagramming, we iteratively drafted a taxonomy with three dimensions on types of harm, risk factors, mechanisms of harm, as well as their connections to one another.

6.2.3 Limitations

This framework is based on a synthesis of existing literature; thus, to some extent we inherit the biases of the literature we rely on. Although we consciously tried to account for this in our literature search, our review may reflect existing knowledge gaps in the literature about specific populations or specific contexts. Like research in the venues we most heavily sampled from, our literature review skewed heavily toward U.S. and European experiences. Our paper collection method, while giving us the flexibility to include work from many different sources, is not exhaustive, and it is possible we have overlooked populations or literature that would expand our taxonomy.

Because many of the studies we draw on are based on participant-reported experiences, harms that are less explainable may have been reported less frequently than they actually occur. For example, harms resulting from automation and data misuse may be underreported because the cause may be difficult to ascertain by the individuals affected.

6.3 A Framework for Risk

		Sensitive information				Societal factors	Targeted attacker			Individual factors			Circumst-antial factors		
Populations	Citations	Intimate media	Known information	Legal status	Health information	Marginalized identity	Government	Intimate	External	Accessibility needs	Low tech literacy	Lack of resources	Celebrity	Moderated access	Social surveillance
Abuse survivors	[26, 249, 314, 325, 233] [152, 187, 79, 284, 311]	●						●				●		●	
Black people	[286, 285, 350, 204, 72] [89, 280, 191, 70, 131]					●	●		●						
Muslim women	[1, 371, 199, 6, 20]	●				●	●		●					●	●
Older adults	[154, 270, 316, 52, 309, 261, 225]				●					●	●			●	
Children	[226, 394, 349]							●		●	●	●		●	
People with stigmatized health conditions	[361, 24, 27, 382, 25, 64]				●	●			●						
People with vision impairments	[138, 188, 11, 15]									●				●	
LGBTQ+ people	[49, 182, 282, 345, 304, 126] [184, 328, 234, 158, 86, 107, 218]			●		●	●		●						
Sex workers	[251, 268, 208, 346, 209, 190] [50, 144, 51, 327, 119]	●		●		●	●		●			●			
Currently/formerly incarcerated people	[291, 331, 287]			●		●	●			●	●	●		●	
Migrants & Refugees	[179, 155, 339, 264, 296]			●		●	●		●		●	●			
Journalists	[257, 195]		●				●		●				●		
Activists	[58, 50, 109, 99]		●				●		●				●		

Table 6.1: Overview of populations studied and their corresponding risk factors.

Through evaluating 82 papers spanning the privacy and security experiences and needs of thirteen different populations, we generated a taxonomy with three dimensions: privacy harms, risk factors, and mechanisms of harm. We first describe *privacy harms*, or the consequences that people face when they experience a privacy violation.

Next, we present the personal and social *risk factors* within and across each population that could lead to privacy harms being more likely or more severe. A summary of the factors each population manages is in Table 6.1.

It is important to note that, while a population may typically have a particular set of risk factors, any individual member of that population may manage fewer or additional risks. Furthermore, Kimberlé Crenshaw's framework for intersectionality demonstrates how each person's experiences of oppression will be unique to their many own identities, rather than simply the sum of its parts [104]. Thus, this taxonomy is not meant to comprehensively represent any person or population's full experience through enumerating risks, but rather offer a broad characterization of the most common and most harmful risks.

Finally, we describe the *mechanisms of harm* we observed in our analysis. These mechanisms are platform policies or features that make it more likely that a risk factor leads to a privacy harm. Risk factors alone cannot result in privacy harms; the technologies that people use can cause or enable these risk factors to become harms based on how the platforms operate. The relationship between risk factors and mechanisms at a high level can be seen in Table 6.2. For example, audience amplification happens by making people and personal data, such as name, home address, criminal records, etc., more accessible or searchable. When this mechanism is encountered by someone with a targeted attacker or experiencing circumstantial factors like being a prominent member of a community, it could make psychological harms and physical harms more likely by empowering an attacker.

In this section, we describe the three dimensions of our taxonomy in detail and discuss how they interact with each other for high-risk populations in particular.

	Risk factors				
Mechanisms	Sensitive information	Marginalized identity	Targeted attacker	Individual factors	Circumstantial factors
Discrimination	●	●		●	
Lack of recourse	●		●	●	
Hard-coded identity	●	●	●		●
Amplification			●		●
Reduced autonomy		●		●	
Unwanted exposure	●	●	●		●
Unwanted access	●		●		●

Table 6.2: Overview of how risk factors and mechanisms interact. For each cell, a circle indicates that a given mechanism makes a risk factor more likely to cause harm.

6.3.1 Privacy Harms

In order to discuss factors that cause or increase risk of harm, we need to establish what a *privacy harm* is. In our review, we identified eight harms: harassment, doxxing, self-censorship, discrimination, social ostracization, violence, financial harm, and loss of agency. Although we approached this work from a different angle—centering high-risk populations—we observed that these categories of harm mapped neatly to Citron and Solove's existing taxonomy of privacy harms [90]; thus, we adopted their terminology.

In this section, we describe each harm and give examples from our review that illustrate the consequences that can occur when high-risk populations experience privacy failures. Throughout the rest of this section, we show how these harms are the outcome of technical mechanisms interacting with risk factors.

Physical Harms Physical harms encompass bodily injury or death. A privacy invasion or the unwanted exposure of information can escalate other risks to physical harm. For example, survivors of intimate partner violence may experience increased violence if their abusers are able to spy on their online activity [152]. Alternatively, if information is revealed unexpectedly to an unwanted audience, such as a person's transgender identity to unaccepting family, this may lead to physical violence against the high-risk person [345]. Similarly, common online abuse such as doxxing and harassment may escalate to violence [251].

Economic Harms Economic harms are financial losses or the reduction in value of something. Economic harms may occur from direct abuse or through the loss of financial opportunity. For example, monetary loss has been frequently reported by older adults, who are more likely to interact with online scams [316]. Alternatively, sex workers who are deplatformed from payment processors face a loss of revenue and threats to their livelihoods (which can also result in physical harm) [251, 50].

Reputational Harms Damage to an individual's reputation and/or standing in the community constitute reputational harms. These harms impair a person's ability to maintain "personal esteem in the eyes of others" [90]. For example, studies on the privacy considerations of Muslim women in the Middle East and North Africa (MENA) discuss participants' concerns about reputational damage that could result for themselves or their families if their social media activity is immoderate or taken out of context, possibly leading to social ostracization [1, 371].

Discrimination Harms This harm is the differential treatment of people based on some personal characteristic such as gender, race, sexual orientation, national origin, age, group membership, or other affiliations. These harms are enacted online as they have been offline, and are characterized by their particular impact on people experiencing oppression or inequality. For example, banks may target people of color with subprime loans based on "race-neutral" Google ad characteristics like home address [276]. Differential treatment can also be the result of holding a stigmatized identity. For example, platforms discriminate against sex workers because of their profession [40]. More generally, platforms can facilitate discrimination by other users through required or accidental disclosure of a sensitive piece of information like HIV status [382]. Discrimination may often overlap with other types of harms. For example, race-based harassment [204] may lead to physical harm or psychological harm, but it also amplifies existing inequalities, making discrimination an additional component of the harm.

Relationship Harms Relationship harms are damage to relationships that are integral to one's life and well-being. For example, LGBTQ+ people may face unaccepting family and ostracization if their identity were accidentally disclosed on social media in an unwanted context [158, 126]. Relationships need not be intimate to have a negative impact when damaged. Research on bias in hiring in the U.S. has shown that having visible indicators of being Muslim on social media reduces call-back rates in deeply conservative areas of the country [6], meaning that unintentional identity disclosure can impact one's ability to find employment and build professional relationships.

Psychological Harms Psychological harms are broad; they encompass both emotional distress and intrusions that "disturb a person's tranquility, interrupt activities, sap time, or serve as a nuisance" [90]. Emotional distress can be triggered by both platforms and by others on the platform [82]. For example, if a trans person is unable to change their name or gender in an online account, the experience of being consistently deadnamed or misgendered can be traumatic [222]. Alternatively, invasions of attention and nuisances can occur through something that is repeatedly disruptive but typically untargeted, such as spam [309] (likely experienced by everyone but reported by older adults), or through highly targeted harassment campaigns designed to inundate the target [195], as may happen to women journalists.

Autonomy Harms Autonomy harms are limitations to or interference with one's ability to make decisions in alignment with their preferences. Citron and Solove define several subcategories of autonomy harms, including coercion, manipulation, failure to inform, thwarted expectations, lack of control, and chilling effects [90]. This level of granularity was not necessary to identify autonomy harms in our literature, and so we do not generally differentiate between the subcategories. In one simple case, autonomy harm may occur when a person's access to the Internet or to devices are monitored by another. For example, when a parent monitors an LGBTQ+ teen's online behavior, they may be chilled from participating in critical identity-forming conversations for fear of being observed by the parent [86]. Alternatively, platforms themselves may reduce the autonomy of their users by offering limited privacy options or delegation tools, as has been reported by older adults and their caregivers [261].

6.3.2 Risk Factors for Privacy Harms

Category	**Risk Factor**	**Definition**
Sensitive protected information	Intimate media	Possession of personal data that one may want control over the exposure of (e.g., intimate photos, browsing history)
	Known information	Possession of information someone else might want (e.g., a journalist knows who their sources are, has leaked docs)
	Legal status	Legal status like criminal history, immigration status, criminalized work or identity
	Health information	Private health information like HIV status, chronic or stigmatized illness
Societal factors	Marginalized identity	Group characteristic (e.g., ethnicity, gender identity, etc) that increases the likelihood of harm. This factor is disbursed across a group rather than targeted to an individual
Targeted Attacker	Government	Government attackers (e.g., police, border patrol) can be generalized as high-resource, low- to sporadic- access
	Intimate	Intimate attackers like a family member or romantic partner have limited resources but high access to devices and personal information; can also be community surveillance
	External	External actors might be strangers who have limited resources and little to no access, but could be highly motivated (e.g., stalker, obsessive fan)
Individual factors	Accessibility needs	Access to accounts and devices may be mediated by accessibility tools or assistance from others
	Low tech literacy	Limited comfort and understanding of technology
	Lack of resources	Limited access to resources that make privacy easier, such as financial or social
Circumstantial factors	Celebrity	Prominence or visibility that may require more caution around exposing personal life details that could be used for doxxing or stalking (e.g., home address, mobile number)
	Moderated digital access	Another person has access to device and accounts, e.g., for the purposes of technical help or intimate surveillance
	Social surveillance	Norm enforcement by community members who do not have direct access to accounts and devices

Table 6.3: Overview of risk factors.

Risk factors are the personal, social, or societal characteristics of a population that make it more likely that they will experience a privacy harm. Our review yielded five broad categories of risk with 14 specific factors. Many of the high-risk populations we investigated had multiple of these factors. These risk factors are defined in Table 6.3 and mapped to the populations we studied in Table 6.1.

The privacy harms that result from each risk factor are highly contextual and often individual. Each risk factor, depending on the person experiencing it, could feasibly lead to any of the harms we identify. Often the combination of risk factors can modulate the ultimate harms experienced by someone. Although we cannot directly connect each risk factor to a discrete set of harms, in this section we highlight harms when they frequently occur as a result of a particular risk factor.

6.3.2.1 Sensitive Protected Information

Being in possession of information one needs to keep private can be a source of risk. The information one holds can be about oneself or about others. For example, journalists may have *known information* (e.g., in the form of leaked documents or their sources' identities) that puts them at risk of targeting by governments, either to obtain access to the information or for retaliation [257]. If an attacker were to gain access to leaked documents, the journalist would suffer relationship harms with their sources, who may not trust them again [257]. Alternately, the information can be personal; for example, *health information* (e.g., HIV status) may be information that someone wants careful control over disclosure [382], as disclosure could lead to relationship harm, reputational harms, or discrimination. Similarly, *intimate media* like photos and videos can be weaponized by abusers who might non-consensually share them to harm the reputation or physical safety of the target [325, 233].

Sensitive information need not be confidential in all contexts. For example, someone may intentionally share intimate media with a romantic partner, while wanting it to stay hidden from others [159]; similarly, *legal status* like immigration status may be disclosed comfortably in community contexts—e.g., through participation in immigrant-support networks—while being kept private in others [179]. Disclosure of a precarious legal status in particular risks the infliction of state violence through search, arrest, or deportation, which can entail further harms such as physical, psychological, discrimination harms [179, 251, 107].

6.3.2.2 Societal Factors

This risk factor broadly refers to group characteristics, like a marginalized identity, which make a person more likely to experience harassment, trolling, or discrimination. In contrast to those with a targeted attacker, people with this risk factor are not being personally targeted, but may nonetheless experience privacy harms related to their identity. This risk factor is particularly closely tied to discrimination harms, which reinforce existing inequalities.

The fact that identity components can be risk factors does not mean that one's identity needs to be concealed. For example, an LGBTQ+ person who has not come out to family may wish to disclose this facet of their identity in some safe online spaces while concealing it on mainstream platforms [182]; alternatively one may choose to be consistently public about an identity for activist and other pro-social purposes, despite the increased likelihood of harassment [234].

6.3.2.3 Targeted Attackers

This type of risk is targeted to a particular individual. In other words, the risk is *specific* rather than *disbursed* across a population, as it may be with harassment or trolling based on an identity characteristic (although these more disbursed attacks can become specific if a particular person is singled out for targeting over time). We identify three subcategories of attackers, each with varying levels of access to the target and resources to conduct the targeting.

A *government* attacker is one with the resources to enact state violence like physical search, deportation, imprisonment, and death, as well as to conduct both targeted and dragnet surveillance. For example, someone with a criminalized identity (e.g., undocumented immigrants [179]) or who does adversarial work on the government (e.g., activists [58] or journalists [257]) may need to keep personal information private from both government surveillance and from corporations who may share information with governments [58]. A government attacker will be highly resourced and may have limited direct access to a target's devices and person (e.g., at the border [251] or through the criminal legal system [291]). In some cases, having a marginalized identity can correspond with experiencing a government attacker. Notably, the New York Police Department conducted extensive surveillance of Muslims in the U.S. after 9/11 based only on religious affiliation and national origin [215], damaging communities (relationships) and chilling speech (autonomy harms) [332].

An *intimate* attacker could be a romantic partner or a family member. This category is characterized by the high level of access the person has to the target's devices, accounts, and physical person. For example, a person with an intimate abuser may have spyware installed on their phone [79], be coerced into sharing passwords with their abuser [152], and may need to worry about the attacker leaking sensitive data like intimate photos to their community to inflict reputational damage [325]. Such surveillance can lead to self-censorship (autonomy harms), physical violence, and psychological harms [152, 249].

An *external* attacker, in contrast, is someone who has little to no direct access to a target, but who nonetheless targets them specifically. For example, women journalists may face targeted harassment or stalking from strangers [195] and staff on political campaigns may be targeted by people looking for damaging material or trying to intimidate the candidate [99].

6.3.2.4 Individual Factors

This category refers to social and/or individual factors that increase access to a person or the likelihood of harm. For example, someone with *lower tech literacy* like an older adult with cognitive impairments may have a more difficult time differentiating real corporate communications from phishing emails, resulting in a higher likelihood of financial harm [261]. Similarly, children, who are not yet fully cognitively developed, may struggle to understand the danger of disclosing personal information online like home address and passwords [226].

Lack of resources may also increase one's risk of privacy invasion. For example, people experiencing homelessness or financial constraints are more likely to use public computers [375, 331] or share personal devices among family members [331]. Someone with financial insecurity, like some sex workers, may also be more likely to compromise security in favor of economic opportunity [251].

Finally, an unmet *accessibility need* can also increase risk of a privacy harm. For example, a CAPTCHA that is designed to be solved by a sighted person can be frustrating or impossible for a low-vision user to complete, blocking their access to content and leading to frustration (psychological harms) and discriminatory treatment [138]. Accessibility needs can also increase the likelihood of harm when combined with other risk factors: if a low-vision person must rely on a spouse or family member to complete online tasks, they may be more vulnerable to intimate attackers [188].

6.3.2.5 Circumstantial Factors

Circumstantial factors are those that are not characteristics of the individual, but dependent on the environment they operate in. For example, multiple populations may have their *access to devices or the Internet managed* by a family member, including older adults [261], children [226], abuser survivors [79], and Muslim women in some regions [199]. Beyond the reduction in autonomy that comes from having a monitored device, the family member may have access to bank accounts, personal communications, and other highly sensitive data [261].

Someone's *prominence* in society or in a particular community, for example as a community leader, journalist, or activist, may also increase the likelihood of their being targeted, and may require a person to be more cautious with personal life details like home address, phone number, etc. For example, an organizer of a protest may be more likely to be targeted, and thus take greater security measures than the typical protester [58].

Social surveillance by community members and peers can be used to enforce social norms, for example on social media. For example, in some communities Muslim women may experience reputational damage or be censured for activity deemed inappropriate by elders [371].

6.3.3 Mechanisms of Harm

In this section, we discuss *mechanisms of harm*, or the technical artifacts and processes that lead risk factors to result in harm in computing environments. While risk factors help us understand *who* is most likely to be harmed and *why*, risk factors alone are usually not enough to result in harm. Harms are caused or enabled through the way that people share information online, interact with platforms, and how platforms themselves dictate the conditions of use. Identifying mechanisms, beyond risks and harms, offers us a novel way to understand *how* harms are enacted and enables us to identify more possible points of intervention. We specifically focus on the role of platforms—including their design, administration, moderation. We identified 14 mechanisms based on the analyzed papers, which we organized into seven categories. These mechanisms are summarized in Table 6.4.

We note again that not every mechanism is unequivocally negative; some mechanisms can be useful for protecting privacy while also threatening privacy. This taxonomy focuses on harms because they are often more difficult to understand and scope than benefits, but researchers and practitioners should consider both when evaluating their work.

Mechanism	Definition
Discrimination	Disparate outcome or treatment caused or enabled by a platform
Algorithmic discrimination	Automated tools leading to disparate impact
Enabled third-party discrimination	Third parties discriminating using the platform features (e.g., with advertising)
Lack of recourse against abuse	Platforms exacerbating or enabling the continuation of abuse through insufficient or missing tools for recourse
Hard-coded identity	Platform-imposed rules on representation that do not meet users' needs
Limits to individual representation	Platforms unduly limiting the ways users can represent themselves
Requirements for identification	Platforms requiring the disclosure of identifying data for access
Audience amplification	Platforms making information more easily searchable; increasing audience of harmful content
Reduced autonomy	Restrictions to users' ability to make informed decisions
Limited control over consumption	When users have little control over the content they are shown or recommended
Coerced data sharing	Platforms limiting user choice to coerce more data sharing
Unwanted exposure	Platforms exposing information to an unintended audience, either mistakenly or intentionally
Exposed to company	A user's data is shared or exposed to a third party against their wishes, or a company infers something private about a user based on intentionally shared data
Exposed to government	A user's data is shared or exposed with a government entity against their will
Exposed interpersonally	A user's data is exposed to someone they know but have attempted to hide the information from
Exposed publicly	A user's data is exposed to the public
Unwanted access	Platforms enabling others to obtain unwanted access to devices or accounts
Accounts vulnerable to intimate attackers	Platforms insufficiently preventing intimate account take-over
Over-privileged access	Platforms failing to offer sufficient account delegation tools

Table 6.4: Overview of mechanisms that cause or enable harms.

6.3.3.1 Discrimination

Discrimination results in disparate treatment based on a risk factor, most frequently a marginalized identity or unmet accessibility needs. Platforms can both enact and facilitate discrimination. Automated systems can, and often do, display bias against groups of people due to biased training data, poor assumptions by designers about what they are evaluating, and by reinforcing existing power structures that disadvantage certain groups of people [46, 280]. For example, face recognition systems have been shown to be less accurate for people with darker skin and for women [70], making it more likely these marginalized groups will be misidentified and face real, offline consequences, such as wrongful arrest from being misidentified by a face recognition algorithm [191].

Some automated systems by their very nature are exclusionary. Automatic Gender Recognition systems are built to sort people into two categories that do not reflect the full breadth of gender expression, creating psychological harms for those who are misgendered and possibly physical risks based on consequences of misgendering (e.g., being forced to prove one's gender to access gendered facilities) [218].

Discrimination may also take the form of disparate impact when a platform insufficiently accommodates the varying needs of its userbase. For example, people with vision impairments may not be able to complete standard text- or image-based CAPTCHAs. These users may be directed to use audio CAPTCHAs instead, which creates an additional burden on these users as audio CAPTCHAs tend to be slower and less accurate [138].

Finally, platforms can also facilitate discrimination by third parties. For example, by making age available to advertisers, companies purchasing ads are empowered to discriminate against older users when advertising jobs [154, 29]. Even when platforms do not let advertisers filter based on sensitive characteristics such as race, having access to characteristics that serve as a proxy for the protected characteristic (e.g., home address for race [276]) may still enable advertisers to discriminate.

6.3.3.2 Lack of Recourse

A lack of recourse often makes other mechanisms more harmful, and can be further amplified when experienced by someone with an individual risk factor such as an unmet accessibility need or lack of resources. When someone experiences harassment, discrimination, doxxing, or other abuse, either from a person or from a platform, a platform can offer multiple ways to assist the user in remedying the harm. When those resources are unavailable, ineffective, or difficult to utilize, the original harm may persist or become worse. For example, sex workers may experience discrimination via account suspension [40, 119] on platforms like AirBnB for being identified as a sex worker, even when they have not used the platform for work. Lack of recourse makes this more severe: when sanctions are enacted for a reason that is not clear to the user or not easily disputable, users are prevented from addressing incorrect inferences. Similarly, shadowbanning (i.e., having content deprioritized or hidden without formal removal or notification) happens to sex workers and activists without transparency, preventing them from remedying the problem [50, 144]. Alternatively, lack of recourse can occur when one is prevented from correcting or retracting previously disclosed information. For example, a person participating on a pregnancy tracking platform may experience a miscarriage. If they are not able to communicate this to the platform, they may be subjected to pregnancy-related advertising and notifications, despite the psychological harm it may cause [64].

Automated systems may make inferences about a user's identity, such as their age or gender. With identity inference especially, the inability for a user to correct the system can be harmful [184]. In a study on trans users' perceptions of automatic gender recognition systems, for example, some participants even suggested that being misgendered by a computer could be more damaging than being misgendered by a person because computer systems are often perceived as objective [184].

6.3.3.3 Hard-coded Identity

Platforms make many decisions around what information to collect, store, and display about their users. When these system design decisions do not account for the many varied ways that people present their identities, and how identities can change over time, they can lead to psychological, reputational, and possibly physical harm. This is a particular concern for those with a marginalized identity and those whose risk factors may lead them to guard personal information like name or location. This could be due to, for example, having a targeted attacker or having other sensitive information they want to talk about while keeping it segregated from their primary online identity, such as legal status or a stigmatized health condition.

"Real name" policies are a good example of how platforms may limit options for self-presentation. Marginalized populations in particular are negatively impacted by bad assumptions about which names are valid, including American Indians [239], drag queens [263], and trans people [112]. Similarly, offering limited gender options can be emotionally harmful for gender non-conforming people and reinforce gender binaries [48]. Forcing a user to choose a single gender globally in a system also risks exposure if they are only partially out with family and friends [182, 86]. Limiting *changes* to name and gender also fails to account for the many ways that people chance their needs and identity over time [182].

Alternatively, requiring the disclosure of certain identifying information like legal name, government identification, email address, or phone number can also create risk for a user. In security advice given to Black Lives Matter protesters, several guides noted how social media companies may work with law enforcement to identify protesters [58], and therefore recommended protesters avoid connecting their legal identification to their accounts and mobile phones. Among sex workers, using separate mobile phones for work and personal business is also common, in part to prevent algorithmic merging of these two identities [251] (with limited success).

6.3.3.4 Amplification

When a person's online presence is made more accessible, or when their content is promoted to new audiences, this can increase the likelihood and severity of harassment, doxxing, stalking, and other antisocial behaviors. This is of particular concern for those with a targeted attacker, as well as those experiencing prominence. For example, phone numbers and email addresses are ubiquitous identifiers online. If a harasser knows this minimal set of information, they may be able to quickly find new platforms their target uses [253, 195]. Platforms that systematically aggregate data can also be particularly risky, because the user has much less control over the information. Adult content platforms, for example, sometimes scrape and republish a sex worker's advertisements from other platforms without the knowledge or consent of the worker [251]. This can increase a sex worker's chances of identification or violence, as they no longer have control over where their content is hosted.

6.3.3.5 Reduced Autonomy

Reduced autonomy refers both to control of one's own information, as well as control over content a user consumes via a platform. This is particularly a concern for people who have personal risk factors like low tech literacy, unmet accessibility needs, and a lack of resources.

For example, platforms can *coerce disclosure* of information from users if they require certain information in order to participate, such as email address, phone number, photo, or government identification. This may be done directly or through the use of "dark patterns," or design decisions that deceive users to act against their own best interests [173]. Once information is disclosed, users may be chilled from speech [86] or from participation for fear of further algorithmic disclosure [25].

Less control over what content one consumes is also a concern for users. For example, studies on privacy concerns of older adults have surfaced that concerns about discriminatory advertising leave them worried about ads online [154]. Lack of input into or ability to opt out from targeted advertising systems can be damaging in many contexts—the promotion of baby product ads after pregnancy loss [25, 64], or of wedding content after a breakup [165], can be a traumatizing experience [82], and there are few mechanisms available to prevent triggering ads.

6.3.3.6 Unwanted Exposure

Unexpected or unwanted exposure of personal information happens when information is shared with an unintended audience. This type of exposure can reveal information that influences others' perception of us or violates social norms [344], and most commonly causes reputational, psychological, and relationship harms. People with sensitive information (e.g., possessing intimate images) or a marginalized identity (e.g., sexual orientation) may experience disproportionate consequences of this mechanism, and those with intimate attackers may be more likely to experience harm due to this mechanism.

Platforms facilitate unwanted or unexpected exposure in multiple ways. We discuss three types of unwanted exposure based on the audience, as the process for information exposure to each of these audiences is different.

Corporate exposure can happen when a platform sells a user's information to a third party or when the platform infers sensitive information about a user that the user did not intentionally disclose. For example, systems that infer the gender of users for targeted advertising may out or misgender trans and gender non-conforming users [184, 218]. Some companies also infer other sensitive information about users: sex workers have extensively documented that online platforms identify their profession and flag their accounts, even when the activity is completely unrelated to their work [50, 119].

Platforms can facilitate exposure of their users to *governments* through compliance with government information requests or by enabling government agencies, or their analytics providers, to access platform activity. For example, the U.S. Immigration and Customs

Enforcement (ICE) has relied on social media data to locate people for deportation [155] and contracts with several social media mining and data analytics companies who have the access and capacity to amass and process large amounts of social media data [296, 264].

Interpersonal exposure happens among people one knows and interacts with, but in an inappropriate context. For example, sex workers have reported having their personal social media promoted to clients, and family suggested to follow work accounts [251]. Both groups of people are intended to have digital connections to the user, but in different contexts. Similarly, LGBTQ+ youth might be algorithmically outed when a platform like Facebook advertises their "likes" of LGBTQ+ media to their family [86].

Exposure to the *public* happens when information becomes available broadly to people the user does not know. This can be particularly risky for someone with social prominence like a celebrity or politician [99], who may have many more people looking for information about them. Someone experiencing targeted harassment or stalking from a stranger, like a journalist [195], may need to take additional measures to prevent doxxing. Similarly, dating apps that depend on geolocation can expose a user's location to many other people and create risks of physical harm [345].

6.3.3.7 Unwanted Access

Data or resources within a person's accounts or devices can also be endangered through unauthorized access by another person. The access can be either totally unauthorized (e.g., account compromise) or through over-privileged access (e.g., family with access to private messages because they share a device with the primary user). This is particularly a concern for people with a targeted attacker.

For example, someone with an intimate abuser may need to worry about the abuser gaining access to their personal accounts. If the account recovery mechanisms rely on information the abuser also knows, like security questions, or if the mobile account owner has full access to all devices on the plan, compromise may be more possible [152].

In other cases, the user may have intentionally given the person access to some accounts for specific purposes, but may lack sufficient account delegation tools to limit access just to that information or context. For example, older adults may seek out tech help from family or services like Geek Squad, and while they have access to do the specific service they may also have access to bank accounts and private messages [154, 270].

6.4 Discussion & Conclusion

We have presented a taxonomy with three dimensions: privacy harms, risk factors, and mechanisms of harm. The relationship between these dimensions helps us understand the relationship between technology and vulnerability across a broad set of populations. Through our review, we identified common privacy harms, 14 risk factors across populations that can lead to harm, 14 mechanisms that enable these risk factors to become harms.

The key insight in our taxonomy is the inclusion of mechanisms. Risk factors alone are not enough to cause harm. It is only in combination with a mechanism that privacy harms result from a risk factor. For example, possession of sensitive data is not in itself dangerous until that information is exposed or stolen. Similarly, having a marginalized identity is not a problem until one must interact with discriminatory algorithms or systems that facilitate harassment. This, in particular, is a strength of this taxonomy: connecting risks to the environments that make them dangerous opens new perspectives for understanding harm and opportunities for intervention.

For example, by highlighting the role of mechanisms in enabling harm, we can see parallels between populations that might otherwise be regarded as dissimilar. Consider "hard-coded identity": perhaps most obviously, limiting the names and genders one is allowed to use on a platform will impact trans people, who may change both fields over time or use multiple versions simultaneously. But we also saw that those with sensitive information may also be harmed by limited options for representation on a platform—perhaps a sex worker must use a pseudonym to defend against legal risks, or a person experiencing pregnancy loss wants to participate anonymously in their online community. Someone with a targeted attacker, like an activist working against a repressive government, may also face harm if they must share a government ID to participate online. Risk factors alone do not convey the common way that these distinct populations may be put in danger. Seeing the number of risk factors, and populations, each mechanism impacts also reveals the vast reach of particular mechanisms, which might otherwise seem to impact a small number of people even if one considers specific high-risk populations.

By thinking about mechanisms as the key part of this taxonomy, we also reframe the conversation around solutions. Rather than framing risk factors as inevitably leading to harm, we instead consider how a risk factor can be exacerbated by the environments in which we operate. This allows us to consider solutions that eliminate the underlying trigger, thus nullifying the "risk" in "risk factor," rather than simply equipping individuals to defend themselves. Of course, for many high-risk populations, the fundamental reason they face risk is societal, such as stigma against LGBTQ+ people, racial and religious marginalization, continued violence against women, increasing hostility toward journalists, among others. Technology cannot solve these problems—this requires societal change. What we can do as technologists, and what this taxonomy helps us do, is to prevent these risks from being triggered online wherever possible. By minimizing harm for the most marginalized users, we stand to benefit *all* users along the way.

6.4.1 Using the Taxonomy

Here we briefly overview several ways that this taxonomy can assist researchers, practitioners, and policy-makers in building safer technology.

For Researchers Researchers can use this synthesis to identify which populations or risk factors are particularly sparse in the literature, as well as the impact of technical mechanisms more broadly. For example, if a mechanism has not yet been documented triggering a particular risk factor, this does not mean that the negative interaction between the two is not present. Researchers studying online safety for particular populations can consider asking about these mechanisms; from this, we can better understand why a population with a particular risk factor is not experiencing harms, for example due to an effective protective measure, or how certain instantiations of the mechanism are more or less likely to lead to harm.

This taxonomy can also provide structure for future research on the privacy needs and practices of high-risk populations. By using this taxonomy of risk factors, harms, and mechanisms as a starting point in new investigations, future research around digital privacy will more systematically cover the landscape of potential privacy risks and more explicitly connect them to vulnerability and risk. This will help privacy and security research as a field build a comprehensive understanding of how different populations experience the same risks and mechanisms, as well as provide researchers a shared language to talk about and compare these risks and mechanisms between populations and contexts.

Finally, by being able to see how the same technical mechanisms lead to harm across populations, researchers can more systematically investigate what protective behaviors are effective at preventing that mechanism from leading to harm. This will not only help us understand how different populations experience harms differently, but can reveal where harms are occurring despite significant effort by communities to prevent them.

For Practitioners For industry practitioners, especially those who build tools used by a wide array of users, understanding the ways technology can harm a variety of users can be time-consuming and challenging. This taxonomy distills the potentially harmful features down to a set of common mechanisms, which can make the work of assessing potential harm more tractable. For any given instantiation of the mechanisms we identified, practitioners should be better equipped to estimate which populations will be most at risk of harm based on the risk factors that interact with the mechanism, reducing the problem space to a manageable level while still covering a wide array of potential problems.

Any of the mechanisms that are present in a system will be there for a reason, and will undoubtedly provide benefits for users and/or the company. Importantly, this framework will help practitioners better reason about potential *negative* impacts of particular design and operational choices, so as to more effectively weigh harms against the known benefits. Further, by increasing our understanding of how these risk factors interact negatively with the mechanisms of a platform, practitioners and researchers alike can work to find new ways to build the most beneficial tools while minimizing harm. Considering the example above, by mapping out the large number of high-risk users who are impacted by systems that require a "hard-coded identity," practitioners will be able to more effectively advocate internally for changes, and have an overview of the digital identity representations that can cause harm.

Furthermore, this taxonomy can be extended. The mechanisms of harm in particular are not exhaustive; new technologies and features may trigger risk factors in novel ways. In developing a mechanism that does not fit well into the existing taxonomy, the framework can be used to interrogate whether the new mechanism might interact in potentially harmful ways with known risk factors, and possibly prompt changes that prevent harm.

For Policymakers Policymakers and regulators stand to impact the online safety of high-risk populations at scale. By looking at harms and mechanisms across many populations, this taxonomy provides a starting point for reasoning about what should be addressed through policy changes rather than through specific technical changes. Our taxonomy provides the connections between mechanisms, harms, and different populations, which will further help policymakers articulate who is most impacted by particular features, and how. For example, allowing third parties to target ads on platforms based on certain demographic features continues to enable discrimination against marginalized groups. Stricter limits on which characteristics platforms are allowed to target on could reduce the need for each platform individually to decide how to address this problem. In that same vein, this taxonomy is a tool that can help demonstrate how far-reaching a particular mechanism is by providing a mapping of mechanisms to risk factors, and an example set of populations that manage those risk factors. This will empower groups advocating for investigation or regulation by revealing the often extensive scope of harm that each of these mechanisms can enable, better conveying the importance and potential impact of change.

6.4.2 Gaps in the Literature—Where Should Researchers Look Next?

The literature available in security and privacy venues skews heavily western. While we explicitly included literature that spanned multiple non-western regions such as the MENA (e.g., [371, 311]), South Asia (e.g., [325, 282]), and Africa (e.g., [109]), this is far from comprehensive. Many U.S. platforms are now reaching a global audience, although not all American platform policies account for the particular needs of populations abroad [40]. Understanding how platform design decisions, features, and data practices impact different populations in context is critical for building safe technology and for ensuring that our solutions do not cause unexpected harm to another population.

One risk factor that was relatively understudied was *prominence*. Through literature on activists and journalists, we were able to identify that being more well-known leads to greater risk of harassment and targeting. There are, however, entire populations for which prominence is a much more central feature, including celebrities and influencers. Further study of these groups could reveal new insight into how *external attackers* operate—i.e., those who are determined but possibly unknown to the target, like an obsessed fan or disgruntled fan.

Finally, this framework decomposes experiences into isolated risk factors, but we know that having multiple intersecting identities leads to unique experiences not fully captured by only understanding each identity alone [104]. There is significant work still to be done on understanding how multiple risk factors combine to make unique harms. This framework can serve as a foundation for this work by providing the core risk factors that people may experience differently in combination.

6.4.3 Conclusion

There has been increasing interest over the last several years in understanding how marginalized and otherwise high-risk populations are experiencing technology, as many face increased risks and outsized consequences when managing a privacy invasion. This framework brings together existing research across multiple disciplines and multiple high-risk communities by taxonomizing common risk factors, privacy harms, and the platform mechanisms that lead these risk factors to result in harms. In doing so, we provide a fuller understanding of how risks are shared across populations, and how they can be triggered by particular platform design decisions. This framework also empowers researchers in finding understudied technologies and risks, technology designers and developers in identifying ways their platforms can be harmful to high-risk populations, and policy-makers in identifying broader patterns in harm across platforms and populations.

CHAPTER VII

Conclusion & Future Work

The Internet has become and will continue to be a critical resource for all people—and serve as both a source of opportunity as well as risk for many. By studying high-risk communities in particular, we stand to better understand where technology designers, developers, and maintainers have overlooked particular needs and experiences, and where there is opportunity for intervention. Through developing safer technology, advocating for more effective regulation, and reforming corporate policy, we will improve digital safety not only for these high-risk communities, but for everyone who uses the Internet.

In this thesis, I bring together several research threads to demonstrate how we can better understand and support digital safety for high-risk populations through multiple methods. First, by conducting in-depth interviews with populations managing significant online risk, we can come to deeply understand their digital privacy and security goals, behaviors, and challenges. In Chapters II and III, I presented work with two specific high-risk populations: undocumented immigrants and sex workers. We observed that although participants in each study took, to varying degrees, privacy-protective behaviors, they struggled to manage risk on platforms that did not meet their specific needs.

Second, by conducting an in-depth investigation into a particular design feature and a large-scale measurement study of unequal access, we are able to better understand the scope and character of particular harmful technologies. In Chapters IV and V, I presented two studies on technical features that create disproportionate harm across users, phone numbers as account identifiers and geoblocking. Through focused study of these mechanisms, we elucidate how technical features lead to privacy, security, and access problems for end-users. In both cases, minor changes to the features stand to make a significant impact on minimizing harms for users.

Finally, by synthesizing these findings and other work on the privacy needs of high-risk populations, we can identify common needs and research opportunities for improving technology across many communities. In Chapter VI, I presented a framework of privacy harms, risk factors, and the technical mechanisms that lead risk factors to result in harm. Combining otherwise isolated work into a meta analysis allows us to see commonalities and patterns across populations and identify broader implications for technology and policy. By bringing together harms for many high-risk populations, we demonstrate that many problems are not only at the margins, but impact a substantial number of people.

7.1 Future Work

Exploring tensions in digital safety needs Our framework demonstrates the many ways that privacy risks overlap across communities and how technical mechanisms can trigger them. However, not every mechanism is uniformly negative, and in fact some populations may benefit from mechanisms that harm others. For example, a platform that limits each user to one account severely restricts the ability of some high-risk groups, like sex workers [251] and LGBTQ+ people [86], to utilize the platform with multiple, deliberately separate social circles. In return, a platform that effectively restricts account access to one account per person may limit harassment through anonymous accounts [360].

Because of the huge diversity of populations and needs across the globe, most solutions will not strictly minimize harm. Thus, when designing solutions and interventions for online safety, researchers and practitioners must reason carefully about the secondary effects of changes. A valuable follow-on work to our framework of privacy risks would be to connect the potential benefits of each mechanism for high-risk populations with the harms, and construct a structured way for researchers an practitioners to reason about trade-offs between risks and benefits.

Measuring corporate policy and legal regulation Corporate policies and government regulation can have a significant impact on whether someone has the tools and resources to protect themselves. For example, the U.S. law FOSTA, which is ostensibly aimed at combating human trafficking, has led many platforms to more aggressively moderate sexual content, globally deplatforming sex workers and making it more difficult for workers to access support communities, safety tools like collaborative bad date lists, and financial security [16, 251, 51]. Research, through identifying the scope and character of harms, can give critical insights to policy decisions before they are made. However, systematic study of the longitudinal impacts of laws and policies after their implementation is also necessary for ensuring the policies are effective.

My work on geoblocking reveals the potential of measurement to enable policymakers and legislators to see the unintentional (or disbelieved) consequences of changes to policy and law. Measurement, broadly defined, can enable us to (1) gather data to demonstrate the impact of a policy on particular communities, making it easier to advocate for change; and (2) better understand the conditions high-risk populations are operating in, so as to make more informed recommendations about individual and community safety strategies.

Policy measurement as a line of future research benefits from having many methods available to answer a broad set of questions. For example, using a method such as large-scale content analysis of community guidelines and terms of service relating to sexual content on major websites, one could observe trends in moderation that help policymakers argue for changes to FOSTA. Such an overview might also help platform users more effectively avoid aggressive moderation by illuminating how moderation in practice differs from written rules. Alternatively, as we continue to see regional privacy laws being enacted with differing scopes and requirements, we may see an increase in the number of websites choosing to geoblock rather than comply with increasingly varied regional laws. Using large-scale network measurements, one can collect and collate longitudinal data on which sites geoblock, where they geoblock, and when they geoblock, better equipping Internet freedom organizations and policymakers to look for versions of privacy regulation that equally support a globally accessible Internet.

Investigating collective privacy Research on understanding safety and protective practices usually focuses on the individual. However, individuals do not operate in isolation; what we know about safety is also based on the experiences and needs of the people we are most connected with. Much of my work so far has been focused on individual behaviors, but we have repeatedly found examples of how community can help safety, and how threats to community can hinder safety. For example, many sex workers rely on community to help vet possibly dangerous clients. For undocumented immigrants, immigrant support communities can pose both a source of assistance and possibly danger, should the community's members be exposed.

Future work could examine how collective safety can be supported by security and privacy tools and strategies. For example, grassroots organizations may face external risks such as surveillance and harassment, while also managing a limited set of resources like time and money. Learning how leadership in such organizations constructs a shared threat model, navigates digital security while achieving other goals, and manages security failures, could provide valuable insights about how existing safety resources do not meet the needs of collectives, as well as reveal strategies that make such communal work effective.

Investigating home-brewed circumvention and safety strategies When faced with an unworkable tool and the need to accomplish a task, people find a way to proceed regardless. Online, this may mean abandoning a security or privacy property they wish they could maintain. But over time, with trial and error and necessity, some people will find creative ways to commandeer or subvert existing mechanisms to serve their needs in a way the tool was not intended to be used. For example, I found that users may circumvent single-account requirements by owning multiple phones, or bypass a paywalled article by loading it in an aggregator site. These "home-brewed" circumvention strategies can be equated to the concept of "desire paths" in urban planning: ways of getting from point A to point B that have not been intentionally architected [278]. These unintended but functioning safety strategies stand to reveal how a particular need is not being met with the tools available, and how the need might be met in the future.

These insights can help us reimagine how we design and build security and privacy tools, which should reflect how people need and intend to use them. For example, in my work I have repeatedly observed strategies for keeping multiple online identities separate from one another. This separation is sometimes done with tricks and unexpected uses of a tool: proactive blocking of family members on an account one does not want them to find; using multiple devices; editing photos so one is unrecognizable and thus unlinkable to another account. A fruitful and challenging line of work is finding an intentional design for multiple, siloed accounts that could relieve the burden of these home-brewed strategies and better align with the needs of real, multifaceted people.

There is a long way to go before all people have equal access to safely participate online. This dissertation demonstrates the value and necessity of centering the experiences and voices of high-risk populations in understanding the current shortcomings of technology and envisioning a more just future. The safer the Internet is for the most marginalized, the safer it will be for all users.

APPENDICES

APPENDIX A

Interview Protocol for "Technology, Risk and Privacy among Undocumented Immigrants"

This is an English version of the protocol we used in Chapter II. One interview was conducted in English and the rest were conducted in Spanish.

A.1 Introduction

We are a team of researchers from the University of Michigan who work on human rights, social change, digital privacy and security. We are are conducting research on the technology practices of undocumented immigrants in the United States and how we can support them support you to use technology to empower and enrich your lives, and to prevent it being used to infringe on your free access to information, expression, privacy, digital security and other liberties.

In this interview, we're hoping to learn how you use technology in your daily lives for information and communication (including computers, mobile phones, social media, and other activities on the Internet), what may be some questions and concerns you have as you use technology needs and concerns, and how we may support you. We will use the findings to develop specific training programs and tools to support members of the community as they navigate the internet and use technology in ways that ensure they can protect themselves and their families online.

The interview will last approximately 1 hour. The general flow of the interview will be:

1. Get to you a little bit
2. Get to know how you use technology and the internet in your daily life
3. Ask about any technology-related concerns you may have for you, your family, your community, etc.
4. Any measures or practices you use to protect your digital information
5. A few closing questions

We will be compensating you $20 for your time. I would like to record this interview to help me remember your responses and use to analyze your responses together with others. To the extent possible, we will ensure that your identity remains completely **confidential**. We will aggregate all the comments from the interviews we're conducting so that your comments are not easily traced to an individual. If we quote you in our final report, we will do so without identifying your name. If there's anything you really don't want on the record, even if it's anonymized, please let me know that, too. Also, this interview is entirely **voluntary** on your part—if for any reason you want to stop, please let me know. We can end the interview at that point with no repercussions for you of any kind. I can also throw out anything you've told me until that point. Is this OK with you? Do you have any questions for me?

I will then start the recording and will ask you to verbally give your consent for participating in this study.

A.2 General Introduction

Some "ice-breaker" questions about their lives (unrelated to tech)

1. Tell us a little bit about yourself.
2. If you're comfortable, we would like to hear about how long you've been in the U.S. and anything you'd like to share about your immigration story, totally optional...
3. Where are you from originally?
4. How long have you been here?
5. How has it been integrating to a new place?
6. Any challenges? Explore...

A.3 Technology in Daily Life

We want to get a sense of how you use technology in your lives.

1. Can you tell me about some of the most common technologies you use on a daily basis?
   (a) How often have you used technology today? What have you used it for? Can you walk us through an example?
   (b) (cellphone, mobile messaging, social media, wikipedia, internet in general, online banking, etc.)
2. For what kinds of purposes?
   (a) To communicate (with whom?)
   (b) To look up information?
   (c) To plan your life/events/work?
   (d) For services (like banking, legal services, shopping, paying bills...?)

3. How/where do you typically use technology? (cell phone? Personal/shared laptop? Public computers?)
4. Do you have internet in your home? A computer in your home?
5. Do you use technology at work?
6. Do you share your devices or accounts with anyone, like partners, children, parents?

A.4 Tech-Related Concerns

1. Have you ever been frustrated with technology recently?
    (a) If so, what happened? [general, to see what comes up]
2. Do you have concerns or worries about your technology use? Tell me about those. [open to all kinds of concerns, not only priv/sec related]
    (a) Look for usability concerns
    (b) Information control concerns
    (c) Tech literacy concerns
    (d) Surveillance concerns (location information, tech-specific concerns, tech used by others (govt, companies, etc.)
    (e) Hacks or other kinds of digital attacks...
3. Have you changed the way you use technology in response to those concerns?
4. Specifically, can you tell me about a recent time when you avoided using a specific technology or platform? [fill in with specific devices, sites, techs types mentioned above]?
5. Are there any information or topics you chose not to discuss or share via tech (communications technologies, social networks, specific devices)?

6. Any specific technologies you avoided? (social media, SMS, email, ..topics you'd prefer not to share via tech?

7. Have there been any (other) events in your life & community or in the broader social/political context that have made you change any of your technology practices?

    (a) *[[explore internal shocks and external shocks. Get answer to what changes, when it changes, and why they think they made those changes]*

    (b) Can you tell me about any specific instances where you have changed your tech practices?

    (c) Are you still doing that now?

8. Has there has ever been a situation where someone gained access to information that you did not want them to have due to technology?

    (a) What happened as a result? What did you do next? How did this experience affect how you use technology? If you made any change in tech use, do you still use that modified behavior today?

When relevant, go through a kind of threat modeling.

1. What may be at risk? What exactly would you want to protect?

    (a) Personal safety and liberty?

    (b) Information about themselves?

    (c) Info about others in a group or network?

    (d) Certain kinds of info?

    (e) Who do you perceive the risk coming from? (Govt in general? ICE specifically?

    (f) Colleagues? Informants? Rival orgs? Companies?

    (g) Any more intimate kinds of third parties (employers, partners, etc))?

2. Who is subject to the risk (themselves vs. community as a whole vs. community members).
3. Why do they perceive this as a risk?
4. What are consequences of the risk if it would become reality?
5. In your view, how likely are these scenarios?
6. If examples come up, probe for examples...

A.5 Group Privacy

1. Do you have concerns or worries about the technology use of anyone in your family or community?
2. Do you worry that the tech behavior of anyone close to you might put you or others in your communities at risk?
3. Can you describe a specific instance where you felt this type of concern?

A.6 Privacy and Security Practices

1. What do you do to try to protect information and communications channels related to any of the topics we just discussed?
   (a) Any choices you make to keep info secure?
2. Can you tell me of the last time you paused to think about and made an adjustment to your tech use as you thought about a potential risk or concern?
3. Have you ever searched for and installed a digital security tool specifically? Why or why not? Would you be willing to?

4. Can you tell me of any specific tools or settings you use?

5. Do you feel like the strategies and tools you're using are effective? Why or why not?

6. Can you tell about any specific technological devices or platforms you trust for certain sensitive topics or communication?

A.7 Tech Knowledge, Resources and Support

1. Where do you get your tech knowledge & support for your work?

2. Have you ever searched for advice online? Are there any specific websites/organizations/resources you've consulted?

3. Have you attended any workshops/trainings?

4. Who do you go when have questions about technology?

A.8 Digital Security Literacy Questions

We'd like to ask you a few questions to see more specifically how you use technology.. This isn't a quiz and there aren't any wrong answers. We just want to know how you use tech! We're also happy to chat about these topics after.

1. What do you consider secure passwords? Do you try to use these?

2. Do you know what two-factor authentication is?

3. Do you use public wifi differently than home/office/school wifi?

4. Have you ever been the victim of a phishing attack?

5. Do you pay attention to the location on your phone and apps?

6. Do you customize privacy settings in certain tools (Google Search, Facebook or online maps)?
7. Do you ever go through the permissions on your phone apps?
8. Would you allow install a plug in...?
9. Do you have any experience with encryption? Can you describe how you use encryption if you do?
10. Do you use any security measures for your phone (lock access? encrypted? Backups?)
11. Do your family members/partners/children know your passwords or unlock pins?
12. Do you avoid having your personal information and media (photos, videos) stored anywhere?

A.9 Follow-up Support

We would like to offer support to you and your community that could make it easier and more effective for you to feel comfortable and secure online and in your tech use.

1. What kind of information or practices would you want to learn in a sec/priv workshop?
2. Do you think workshop, training, walk-in session to support with tech and security would be of interest and useful?
3. In-person training / workshop vs. resources (e.g. printed leaflet with best practices): what would be more useful?
4. Any other ideas?

We would like to conduct interviews with other undocumented immigrants to learn about their own technology practices, their perspectives on risks when using technology or connecting online, and what they do (or may be interested in doing/not doing) to be safer. Would you be able to share our recruitment flier with others and ask them to consider participating?

Any questions about technology we talked about today?

Thank you so much for participating. Here is $20 for your time and participation.

APPENDIX B

Interview Protocol for "Safety is More than Security"

B.1 Introduction

Thank you for taking the time to talk to us. First, let's quickly go over how today's study is going to work. I'm going ask you questions about your use of technology and experiences that you have had both on technology and in your general life. I expect that our conversation will take approximately one hour. You can feel free to let me know if you don't want to answer any questions, and we'll move on to the next question or we can stop the study.

B.2 Employment

I would like to begin with a few questions about your job.

1. Could you tell me a little bit about what you do as your profession?
    (a) [if they did not describe sex work] Could you tell me more about the sex work that you do?
    (b) How long would you say you've been doing this?

2. What devices do you use to access the internet (tablet, mobile phone, laptop, desktop computer, something else)?
    (a) Would you say that there is one you use most often (that you would consider your primary device)?

B.3 Internet Use in Personal Life

I'd like to start our conversation with a discussion of how you typically use the internet.

1. When did you first start using the Internet or a mobile phone?
2. What do you usually do online during your free time (when you're not working)?
    (a) Do you use social media at all (Facebook, Instagram, Twitter, Pinterest, Snapchat, Whisper)? Chat? Read articles? Post articles? Share or view pictures?
    (b) [prompts] do you seek out information online like searching for entertainment or news?
    (c) [prompts] do you play games online or on your phone or a gaming console?
    (d) [prompts] do you post on forums
    (e) [prompts] do you have your own website or blog
3. What portion of your free time would you say that you spend online or using your mobile phone?
4. Overall, would you say you enjoy spending time online?
    (a) Why / why not?

B.4 Internet Use for Work

Next I'd like to talk about how you use the Internet for your sex work.

1. How do you advertise your services?

    (a) Do you use the internet to advertise?

    (b) Do you post online ads, do you have your own website, use clips sites, use social media

    (c) If yes:

        i. How did you learn that it was possible to find clients this way?

        ii. How did you learn how to use these services?

        iii. Were there any particular challenges you ran into?

        iv. What makes you more or less likely to use a particular advertising site

        v. Does it matter whether the site requests personal information?

    (d) If not:

        i. Why not? How do you advertise instead?

        ii. Is this how you've always advertised / did you do it differently in the past?

2. Do you do anything to screen clients?

    (a) If yes, how? [prompt: What sources do you use? Do you use the internet?]

    (b) If not: have you considered doing so? Why did you stop / decide not to?

    (c) Did you have any challenges when trying to find a screening method?

3. How do you maintain relationships with your clients?

    (a) Where are you connected with your clients? Email, SMS, Whatsapp, Signal, Twitter, Switter, Facebook, etc.

    (b) How did you decide to select these services? [prompts] disappearing messages, end-to-end encryption, sufficient ability to block

    (c) Are there any ways in which you restrict your communications? [prompts] time spent, information shared?

   (d) Have you ever adapted your practices to what a client wanted to use? Has a client ever made requests for "safer" tools or ways of communicating?

4. How do clients pay you? [Payment processing]

   (a) How did you decide what payment method to use?

   (b) Have you always used this payment method?

   (c) Did you have any challenges when selecting a payment method?

   (d) [if not mentioned] is how much information is revealed to your client or the payment provider a concern?

   (e) [if not mentioned] Have you ever heard of bitcoin? If yes, have you considered using bitcoin?

5. Do you use the internet to talk to other people working in the sex industry?

   (a) Where? [What resources do you use?]

   (b) How did you find these resources?

   (c) Would you say this is the primary place where you talk about your work / find support?

      i. Has this always been true?

6. Are there other ways that we have not talked about in which you use the internet for your work?

   (a) [prompts] online forums, connecting with others

7. Overall, how important would you say the Internet is for your business?

8. How did you learn all of these online practices?

   (a) How did you decide to follow the advice/recommendation/suggestion?

9. Has your use of the Internet changed over the time you've been doing sex work? How?

10. What are aspects of your work that current tools and services cannot help with even though you wish they could? [Are there any online tools you wished existed for you to use in your work? What would those look like, what would they do?]

B.5 Persona Separation

Some people try to maintain distance between their personal and work life, others don't.

1. Do you try to separate your work and personal content online? Or in general? or do you feel like it's all one and the same?

   (a) If separate:

      i. What exactly does this entail? Separate profiles? Separate devices?

      ii. Would you say that you try to "be a certain person" or maintain a particular "image" when using the internet for your [work/personal]?

      iii. Why did you decide to keep things separate?

      iv. Were there any challenges?

      v. Are there any particular tools or settings that you use?

      vi. Would you be upset if there was overlap or if a client found your personal content?

      vii. Has this worked or have you had any cases where things did not work out as you would have liked?

   (b) If not separate, why not?

2. Have you always done it this way? Why?

3. Overall, what does privacy mean for you? How would you define privacy?

B.6 Threat Models

Now I'd like to talk a little bit about your online experiences, in both your work and personal life.

1. Have you ever had anything you would consider a negative experience online?

2. [if they already mentioned an experience in this category, ask about any other experiences and if this category is something they're actively concerned about] In your personal life, do you have any concerns about your accounts?

   (a) [prompts] someone accessing or using your accounts? Losing money / financial consequences? Finding out any information? Being harassed or bullied?

   (b) [for a person] Why would you be concerned about [this person gaining access/this happening]?

      i. What would you be concerned about them finding?

      ii. What would you be concerned about them doing?

   (c) Has anything like this ever happened?

      i. If yes: How do you think this happened? (how did someone get into your account?)

   (d) What were the resources available for you to prevent this?

      i. How/why/where did you learn this?

      ii. How did you decide it was a good idea / why did you listen?

   (e) Is there anything you've considered doing or think might be a good idea to do for protection but don't do right now?

      i. Do you ever worry about these issues?

         A. If yes, how often?

         B. How seriously are you concerned about such issues happening?

3. Have you ever had anything you would consider a negative experience related to your work, online?

    (a) [prompts] having a client find out something about you that you didn't want them to know? For example, finding real names or phone numbers? Threatening text? Blackmail? (Doxxing)

4. Have you ever had any unintended crossing over of your "work" and "personal" lives?

    (a) [prompts] Clients recommended to you on Facebook? Friends/family being recommended to follow your work social media? Receiving advertisements for work products on personal computer? Having people you know see your advertisements?

    (b) How/why do you think this happened? (how was info found by wrong person, why does fb recommend those people, Instagram to Facebook suggested follows...)

    (c) Were you interested in trying to prevent this in the future?

    (d) Do you ever worry about these issues?

        i. How seriously are you concerned about such issues happening?

5. In general, what would you say are your online security or privacy concerns? [do you have any concerns [security / privacy worries] that we have not discussed?]

6. Would you say you're more concerned about someone you know or someone you don't know gaining access to an account?

    (a) Why?

7. How about gaining access to your information?

    (a) Why?

B.7 Safety

Now I'd like to talk a little bit about how you stay safe online, both in your personal and work life.

1. What is Safety to you as a sex worker? How do you define Safety?
2. Would you say you do anything in particular to maintain your safety online?
   (a) In your personal life? In work life?
   (b) What do you do?
   (c) How did you decide to do these things?
   (d) Where did you learn them? Why did you decide they were a good idea?
3. Would you say that you use strong passwords / good password practices?
   (a) Why / why not?
   (b) Do you do anything different for your personal and work accounts? Why / why not?
   (c) How did you learn about doing this? How did you decide it was a good idea / why did you listen?
   (d) Would you say you do anything else to protect your security?
   (e) Have you ever set up an account so that you have to enter a code that came to your phone in order to get into an online account? (Do you use 2FA.)
   (f) Have you ever changed your password settings (or have you changed your security behavior over time)? [If yes] What prompted the change?
4. Do you typically customize the privacy settings for your online accounts?
   (a) How do you customize them?

    (b) Is there any account where you take special care with privacy settings? Why/why not?

    (c) Do you do anything different for your personal and work accounts? Why/why not?

    (d) How did you learn about doing this? How did you decide it was a good idea / why did you listen?

    (e) Would you say you do anything else that you think helps protect your privacy?

    (f) Would you say that you avoid saying certain things online?

        i. Why/why not?

        ii. Has this changed over time?

    (g) Have you ever had to block someone? Or have you deactivated an account?

    (h) Have you changed how you approach privacy at all over time? [If yes] What prompted the change?

5. Have you ever suspected (or been told by your account) that someone was trying to log in to your account?

    (a) Who did you think was trying to get in?

    (b) How concerned did you feel about that?

    (c) Was it more concerning that this was a [personal/work] account rather than a [work/personal] account? Why?

    (d) Did you do anything differently afterwards?

6. [if not covered] Have you ever had to block someone? Or have you deactivated an account?

7. Have you ever felt harassed [bullied] online?

(a) Can you tell me a little bit about what happened?

(b) Why do you think this happened?

(c) How intense was this experience?

(d) Were you interested in trying to prevent this in the future?

i. Were any specific measures available for you to try to prevent this?

ii. How/why/where did you learn this? How did you decide it was a good idea / why did you listen?

(e) [if not work related] How about in your [work/personal] life?

(f) Would you say that you do anything in general to avoid harassment?

8. Overall, would you say that you try to do the same types of things for your work and personal accounts / internet uses?

(a) Why [same/different]?

(b) Has it always been like this, if not, what made you change?

(c) If different: which is more important?

B.8 Learning

1. In general, where or from whom have you learned strategies for protecting yourself online?

(a) [prompts] other sex workers, library, online forums, online websites, friends, family, other type of work

(b) Any different sources for work or for personal?

2. How do you decide who is a good source for learning/tips?

3. Have you changed how you look for information over time?

4. Would you say that you actively seek out information or keep tabs on this information, or more that you pick it up if it comes to you?

B.9 Online vs. Offline Safety

1. In your work life, would you say you're more concerned about safety in the offline world (like getting physically hurt) or safety online?
   (a) Why?
   (b) Do you think these two are connected in any way?
   (c) How so? What makes you think this?
   (d) Have you always felt this way?

B.10 Pre- and Post-Sex Work Reflections

1. Would you say that working in the sex industry has changed your concerns online?
   (a) How about in the offline world?
   (b) How do you feel about this change?
2. Do you think that working in the sex industry has changed how you behave online?
   (a) How about in the offline world?
   (b) How do you feel about this change?

B.11 Anything Else

1. If you were to give new people doing your type of sex work advice about using the Internet for their work, what would you tell them?

2. In general, what advice would you offer to people about staying safe? (And how about staying safe online?)

3. Is there anything else that you have not had a chance to mention, or that you would like to share with us or that you think we should know?

B.12 Conclusion

Thank you very much for speaking with me today. Here is your code for your [giftcard].

APPENDIX C

Survey Questions From “Perils of a Universal Identifier”

Q1: Please select all types of phone numbers you have had in the last 5 years.

- Mobile phone number
- Landline (i.e. household number)
- Virtual phone number (e.g. Google Voice, Skype number)

Q2: Do you have your own mobile phone or do you share it with someone else?

- I have my own mobile phone
- I share a mobile phone

[Conditional] **Q3**: Who do you share a mobile phone with?

- My spouse / partner
- My parent(s)
- My sibling(s)
- My children
- Other: [free response]

Q4: How many times have you gotten a new phone number in the last 5 years?

- 0 times
- 1 time
- 2-5 times
- 5+ times

Q5: How long have you had your current primary phone number (in years)?

[Drop down of items from 1 year to 10 years]

Q6: Have you had any annoying, weird, or disturbing experiences involving your phone number? Please describe your experience in as much detail as possible. Feel free to write about as many experiences as you wish.

Q7: Were there any consequences for you because of the experiences you described above (e.g., with respect to your privacy, safety or ability to access services)? Please explain.

Q8: Have you ever been unable to use an online service, app or other resources because you could not provide a phone number? If yes, please 1) explain what happened and 2) describe any consequences for you.

Q9: Have you ever lost access to a phone number (e.g. because you couldn't pay your cellular bill)? If yes, please 1) explain what happened and 2) describe any consequences for you.

Q10: Have you ever had any weird experiences with phone number recycling (e.g. getting a number that was previously owned by someone else)? If yes, please 1) explain what happened and 2) describe any consequences for you.

Q11: Have you had any experiences in which you had to share your phone number with an online service, an app, a company, or a person but felt uncomfortable doing so? If yes, please 1) explain why you were uncomfortable and 2) what any consequences were for you.

Q12: If these questions jogged your memory about any other negative experiences with phone numbers that you have not yet shared, please tell us about the experiences and the consequences here.

Q13: In which country do you currently live?

[Drop down of list of countries]

Q14: What is your age?

- 18-24
- 25-34
- 35-44
- 45-54
- 55-64
- 65 or older
- Prefer not to answer

Q15: What is your gender?

- Male
- Female
- Nonbinary
- Other: [free response]
- Prefer not to answer

Q16: 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)
- Prefer not to answer

Q17: Which statement best describes your current employment status?

- Employed full-time (working 40 or more hours per week)
- Employed part-time (working up to 39 hours per week)
- Not working (looking for work)
- Not working (not currently looking for work)
- Self-employed
- Homemaker
- Retired
- Student
- Unable to work
- Prefer not to answer

BIBLIOGRAPHY

BIBLIOGRAPHY

[1] Norah Abokhodair and Sarah Vieweg. Privacy & social media in the context of the arab gulf. In *Proceedings of the 2016 ACM Conference on Designing Interactive Systems*, DIS '16, page 672–683, New York, NY, USA, 2016. Association for Computing Machinery.

[2] Ruba Abu-Salma, Elissa M Redmiles, Blase Ur, and Miranda Wei. Exploring user mental models of end-to-end encrypted communication tools. In *8th USENIX Workshop on Free and Open Communications on the Internet (FOCI 18)*, 2018.

[3] Ruba Abu-Salma, M. Angela Sasse, Joseph Bonneau, Anastasia Danilova, Alena Naiakshina, and Matthew Smith. Obstacles to the Adoption of Secure Communication Tools. In *2017 IEEE Symposium on Security and Privacy (SP)*, 2017.

[4] Alessandro Acquisti, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie Faith Cranor, Saranga Komanduri, Pedro Giovanni Leon, Norman Sadeh, Florian Schaub, Manya Sleeper, Yang Wang, and Shomir Wilson. Nudges for privacy and security: Understanding and assisting users' choices online. *ACM Comput. Surv.*, 50(3):44:1–44:41, August 2017.

[5] Alessandro Acquisti, Laura Brandimarte, and George Loewenstein. Privacy and human behavior in the age of information. *Science*, 347(6221):509–514, 2015.

[6] Alessandro Acquisti and Christina Fong. An experiment in hiring discrimination via online social networks. *Management Science*, 66(3):1005–1024, Nov 2019.

[7] Alessandro Acquisti, Leslie K John, and George Loewenstein. What is privacy worth? *The Journal of Legal Studies*, 42(2):249–274, 2013.

[8] The Social Security Administration. Identity theft and your social security number, 2018. `https://www.ssa.gov/pubs/EN-05-10064.pdf`, accessed 2020-08-15.

[9] North American Numbering Plan Administrator. April 2019 north american numbering plan (nanp) exhaust analysis, April 2019. `https://nationalnanpa.com/reports/April_2020_NANP_Exhaust_Analysis%20Final.pdf`, accessed 2020-09-02.

[10] Syed Ishtiaque Ahmed, Md. Romael Haque, Jay Chen, and Nicola Dell. Digital privacy challenges with shared mobile phone use in bangladesh. *Proc. ACM Hum.-Comput. Interact.*, 1(CSCW):17:1–17:20, December 2017.

[11] Tousif Ahmed, Patrick Shaffer, Kay Connelly, David Crandall, and Apu Kapadia. Addressing physical safety, security, and privacy for people with visual impairments. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, pages 341–354, Denver, CO, June 2016. USENIX Association.

[12] American Airlines. BeNotified, no date. https://www.aa.com/i18n/travel-info/travel-tools/benotified.jsp, accessed 2020-08-26.

[13] Akamai. Akamai pragma header. https://community.akamai.com/customers/s/article/Akamai-Pragma-Header?language=en_US.

[14] Kona DDoS Defender. https://www.akamai.com/us/en/resources/cdn-ddos.jsp.

[15] Taslima Akter, Bryan Dosono, Tousif Ahmed, Apu Kapadia, and Bryan Semaan. "i am uncomfortable sharing what i can't see": Privacy concerns of the visually impaired with camera based assistive applications. In *29th USENIX Security Symposium (USENIX Security 20)*, pages 1929–1948. USENIX Association, August 2020.

[16] Kendra Albert, Emily Armbruster, Elizabeth Brundige, Elizabeth Denning, Kimberly Kim, Lorelei Lee, Lindsey Ruff, Korica Simon, and Yueyu Yang. Fosta in legal context. Available at SSRN: https://ssrn.com/abstract=3663898, 2020.

[17] Sean T Allen, Katherine HA Footer, Noya Galai, Ju Nyeong Park, Bradley Silberzahn, and Susan G Sherman. Implementing targeted sampling: lessons learned from recruiting female sex workers in baltimore, md. *Journal of Urban Health*, 96(3), 2019.

[18] Hazim Almuhimedi, Florian Schaub, Norman Sadeh, Idris Adjerid, Alessandro Acquisti, Joshua Gluck, Lorrie Faith Cranor, and Yuvraj Agarwal. Your location has been shared 5,398 times!: A field study on mobile app privacy nudging. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, CHI '15, pages 787–796, New York, NY, USA, 2015. ACM.

[19] Irwin Altman. *The environment and social behavior: privacy, personal space, territory, crowding*. Brooks/Cole Pub. Co, 1975.

[20] Maha Aly. Promoting usability and ux design for more inclusivity of muslim residents and refugees within non-muslim communities. CHI Extended Abstracts, 2020.

[21] Tawfiq Ammari, Priya Kumar, Cliff Lampe, and Sarita Schoenebeck. Managing children's online identities: How parents decide what to disclose about their children online. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, CHI '15, pages 1895–1904. ACM, 2015.

[22] Deborah Amos. Lebanon's government is accused of swarming whatsapp to catch protesters, 2020. https://www.npr.org/2020/03/09/809684634/lebanons-government-is-accused-of-swarming-whatsapp-to-catch-protesters, accessed 2020-09-01.

[23] amp/aw. EU parliament bans geoblocking, exempts Netflix and other streaming services, Feb 2018. http://www.dw.com/en/eu-parliament-bans-geoblocking-exempts-netflix-and-other-streaming-services/a-42475135.

[24] Nazanin Andalibi. Disclosure, privacy, and stigma on social media: Examining non-disclosure of distressing experiences. *ACM Trans. Comput.-Hum. Interact.*, 27(3), may 2020.

[25] Nazanin Andalibi and Patricia Garcia. Sensemaking and coping after pregnancy loss: The seeking and disruption of emotional validation online. *Proc. ACM Hum.-Comput. Interact.*, 5(CSCW1), apr 2021.

[26] Nazanin Andalibi, Oliver L. Haimson, Munmun De Choudhury, and Andrea Forte. Understanding social media disclosures of sexual abuse through the lenses of support seeking and anonymity. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, CHI '16, page 3906–3918, New York, NY, USA, 2016. Association for Computing Machinery.

[27] Nazanin Andalibi, Margaret E. Morris, and Andrea Forte. Testing waters, sending clues: Indirect disclosures of socially stigmatized experiences on social media. *Proc. ACM Hum.-Comput. Interact.*, 2(CSCW), nov 2018.

[28] Nathanael Andrews. "can i get your digits?": Illegal acquisition of wireless phone numbers for sim-swap attacks and wireless provider liability. *Nw. J. Tech. & Intell. Prop.*, 79, 2018.

[29] Julia Angwin, Noam Scheiber, and Ariana Tobin. Dozens of companies are using facebook to exclude older workers from job ads. ProPublica, December 2017. https://www.propublica.org/article/facebook-ads-age-discrimination-targeting, accessed 2022-04-02.

[30] Anonymous. Towards a comprehensive picture of the Great Firewall's DNS censorship. In *4th USENIX Workshop on Free and Open Communications on the Internet (FOCI)*, 2014.

[31] Apple. Hide my email for sign in with apple, December 2020. https://support.apple.com/en-us/HT210425, accessed 2020-01-08.

[32] Apple. Using dual sim with an esim, November 2020. https://support.apple.com/en-us/HT209044, accessed 2020-08-03.

[33] Payal Arora. Decolonizing Privacy Studies. *Television and New Media*, 20(4), 2019.

[34] Simurgh Aryan, Homa Aryan, and J Alex Halderman. Internet censorship in Iran: A first look. In *3rd USENIX Workshop on Free and Open Communications on the Internet (FOCI)*, 2013.

[35] Assembly Four. Empowering sex workers through technology. https://assemblyfour.com, accessed 2021-02-16.

[36] Austrlian House Standing Committee on Infrastructure and Communications. At what cost? IT pricing and the Australia tax, July 2013. https://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=ic/itpricing/report.htm.

[37] Susan B. Barnes. A privacy paradox: Social networking in the united states. *First Monday*, 11(9), 2006.

[38] Luis Fernando Baron and Ricardo Gomez. Living in the limits: Migration and information practices of undocumented latino migrants. In Jyoti Choudrie, M. Sirajul Islam, Fathul Wahid, Julian M. Bass, and Johanes Eka Priyatma, editors, *Information and Communication Technologies for Development*, 2017.

[39] Luis Fernando Baron, Moriah Neils, and Ricardo Gomez. Crossing new borders: computers, mobile phones, transportation, and english language among hispanic day laborers in seattle, washington. *Journal of the Association for Information Science and Technology*, 65(1):98–108, 2014.

[40] Catherine Barwulor, Allison McDonald, Eszter Hargittai, and Elissa M Redmiles. “Disadvantaged in the American-dominated internet”: Sex, Work, and Technology. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, 2021.

[41] BBC News. GDPR: US news sites unavailable to EU users under new rules, May 2018. https://www.bbc.com/news/world-europe-44248448.

[42] Frank D Bean, Susan K Brown, and James D Bachmeier. *Parents without papers: The progress and pitfalls of Mexican American integration*. Russell Sage Foundation, 2015.

[43] Adam Beautement, M Angela Sasse, and Mike Wonham. The compliance budget: managing security behaviour in organisations. In *Proceedings of the 2008 New Security Paradigms Workshop*, 2008.

[44] Alvaro M. Bedoya. Deportation is going high-tech under trump. *The Atlantic*, June 2017. [Online; Retrieved 17 September 2017].

[45] Ali Behdad. *A Forgetful Nation: On Immigration and Cultural Identity in the United States*. Duke University Press, 2005.

[46] Ruha Benjamin. *Race After Technology: Abolitionist Tools for the New Jim Code*. John Wiley & Sons, Medford, MA, USA, 2019.

[47] Andrew Besmer and Heather Richter Lipford. Moving beyond untagging: Photo privacy in a tagged world. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI ’10, pages 1563–1572, New York, NY, USA, 2010. ACM.

[48] Rena Bivens and Oliver L. Haimson. Baking gender into social media design: How platforms shape categories for users and advertisers. *Social Media + Society*, 2(4):2056305116672486, 2016.

[49] Lindsay Blackwell, Jean Hardy, Tawfiq Ammari, Tiffany Veinot, Cliff Lampe, and Sarita Schoenebeck. Lgbt parents and social media: Advocacy, privacy, and disclosure during shifting social movements. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, CHI '16, page 610–622, New York, NY, USA, 2016. Association for Computing Machinery.

[50] Danielle Blunt, Emily Coombes, Shanelle Mullin, and Ariel Wolf. Posting into the void: Studying the impact of shadowbanning on sex workers and activists, 2020.

[51] Danielle Blunt and Ariel Wolf. Erased - the impact of fosta-sesta and the removal of backpage, 2020.

[52] Linda Boise, Katherine Wild, Nora Mattek, Mary Ruhl, Hiroko H. Dodge, and Jeffrey Kaye. Willingness of older adults to share data and privacy concerns after exposure to unobtrusive in-home monitoring. *Gerontechnology: international journal on the fundamental aspects of technology to serve the ageing society*, 11(3):428–435, 2013.

[53] J. Bonneau, C. Herley, P. C. v. Oorschot, and F. Stajano. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *2012 IEEE Symposium on Security and Privacy*, pages 553–567, USA, 2012. IEEE.

[54] Joseph Bonneau, Cormac Herley, Paul C. van Oorschot, and Frank Stajano. Passwords and the evolution of imperfect authentication. *Communications of the ACM*, 58(7), 2015.

[55] Nikita Borisov, Ian Goldberg, and Eric Brewer. Off-the-record communication, or, why not to use pgp. In *Proceedings of the 2004 ACM Workshop on Privacy in the Electronic Society*, WPES '04, pages 77–84, New York, NY, USA, 2004. ACM.

[56] Christoph Bösch, Benjamin Erb, Frank Kargl, Henning Kopp, and Stefan Pfattheicher. Tales from the dark side: Privacy dark strategies and privacy dark patterns. *Proceedings on Privacy Enhancing Technologies*, 2016(4):237–254, 2016.

[57] danah boyd. *It's Complicated: The Social Lives of Networked Teens*. Yale University Press, 2014.

[58] Maia J. Boyd, Jamar L. Sullivan Jr., Marshini Chetty, and Blase Ur. Understanding the security and privacy advice given to black lives matter protesters. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, CHI '21, New York, NY, USA, 2021. Association for Computing Machinery.

[59] Laura Brandimarte, Alessandro Acquisti, and George Loewenstein. Misplaced confidences: Privacy and the control paradox. *Social Psychological and Personality Science*, 4(3):340–347, 2013.

[60] Russell Brandom. The us border patrol is trying to build face-reading drones, April 2017. [Online; Retrieved 17 September 2017].

[61] Russell Brandom. The frighteningly simple technique that hijacked jack dorsey's twitter account. The Verge, August 2019. `https://www.theverge.com/2019/8/31/20841448/jack-dorsey-twitter-hacked-account-sim-swapping`, accessed 2020-08-27.

[62] Virginia Braun and Victoria Clarke. Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2):77–101, 2006.

[63] T. Bray. An HTTP status code to report legal obstacles, February 2016.

[64] Gillian Brockell. Dear tech companies, i don't want to see pregnancy ads after my child was stillborn, December 2018. `https://www.seattletimes.com/life/dear-tech-companies-i-dont-want-to-see-pregnancy-ads-after-my-child-was-stillborn/`, last accessed 2022-04-13.

[65] Susan K. Brown and Alejandra Jazmin Sanchez. Parental legal status and the political engagement of second-generation mexican americans. *RSF: The Russell Sage Foundation Journal of the Social Sciences*, 3(4):136–47, 2017.

[66] Finn Brunton and Helen Nissenbaum. *Obfuscation*. The MIT Press, USA, 2015.

[67] Andreas Buchenscheit, Bastian Könings, Andreas Neubert, Florian Schaub, Matthias Schneider, and Frank Kargl. Privacy implications of presence sharing in mobile messaging applications. In *Proceedings of the 13th International Conference on Mobile and Ubiquitous Multimedia*, MUM '14, pages 20–29, New York, NY, USA, 2014. ACM.

[68] BuiltWith. Akamai usage statistics. `https://trends.builtwith.com/cdn/Akamai`.

[69] Frauen und Jugend Bundesministerium für Familie, Senioren. The new prostitute protection act, 2019. `https://www.bmfsfj.de/blob/117624/ac88738f36935f510d3df8ac5ddcd6f9/prostschg-textbausteine-en-data.pdf`, accessed 2020-10-03.

[70] Joy Buolamwini and Timnit Gebru. Gender shades: Intersectional accuracy disparities in commercial gender classification. In Sorelle A. Friedler and Christo Wilson, editors, *Proceedings of the 1st Conference on Fairness, Accountability and Transparency*, volume 81 of *Proceedings of Machine Learning Research*, pages 77–91. PMLR, 23–24 Feb 2018.

[71] Jenna Burrell and Ken Anderson. 'i have great desires to look beyond my world': trajectories of information and communication technology use among ghanaians living abroad. *New Media & Society*, 10(2):203–224, 2008.

[72] Jim Campen. The color of money in greater boston: Patterns of mortgage lending and residential segregation at the beginning of the new century, January 2004.

[73] Tammy Castle and Jenifer Lee. Ordering sex in cyberspace: A content analysis of escort websites. *International Journal of Cultural Studies*, 11(1), 2008.

[74] Ricardo Castro-Salazar and Carl Bagley. 'ni de aqui ni from there': Navigating between contexts: Counter-narratives of undocumented mexican students in the united states. *Race Ethnicity and Education*, 13(1):23–40, 2010.

[75] Pew Research Center. Mobile fact sheet, June 2019. `https://www.pewinternet.org/fact-sheet/mobile`, accessed 2020-08-23.

[76] Abdelberi Chaabane, Terence Chen, Mathieu Cunche, Emiliano De Cristofaro, Arik Friedman, and Mohamed Ali Kaafar. Censorship in the wild: Analyzing Internet filtering in Syria. In *14th ACM Internet Measurement Conference (IMC)*, 2014.

[77] Lura Chamberlain. Fosta: A hostile law with a human cost. *Fordham Law Review*, 87(5), 2019.

[78] Daphne Chang, Erin L. Krupka, Eytan Adar, and Alessandro Acquisti. Engineering information disclosure: Norm shaping designs. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, CHI '16, pages 587–597, New York, NY, USA, 2016. ACM.

[79] Rahul Chatterjee, Periwinkle Doerfler, Hadas Orgad, Sam Havron, Jackeline Palmer, Diana Freed, Karen Levy, Nicola Dell, Damon McCoy, and Thomas Ristenpart. The spyware used in intimate partner violence. In *2018 IEEE Symposium on Security and Privacy (SP)*, pages 441–458, 2018.

[80] Leo R. Chavez. *Shadowed Lives: Undocumented Immigrants in American Society*. Wadsworth, third edition, 2012.

[81] Brian X. Chen. I shared my phone number. i learned i shouldn't have. The New York Times, August 2019. `https://www.nytimes.com/2019/08/15/technology/personaltech/i-shared-my-phone-number-i-learned-i-shouldnt-have.html`, accessed 2020-08-10.

[82] Janet X. Chen, Allison McDonald, Yixin Zou, Emily Tseng, Kevin A. Roundy, Acar Tamersoy, Florian Schaub, Thomas Ristenpart, and Nicola Dell. Trauma-informed computing: Towards safer technology experiences for all. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, CHI '22, New York, NY, USA, 2022. Association for Computing Machinery.

[83] Jay Chen, Michael Paik, and Kelly McCabe. Exploring internet security perceptions and practices in urban ghana. *In Proc. Symposium on Usable Privacy and Security (SOUPS '14)*, 14, 2014.

[84] Wenli Chen. Internet-usage patterns of immigrants in the process of intercultural adaptation. *Cyberpsychology, Behavior, and Social Networking*, 13(4):387–399, 2010.

[85] Wenli Chen and Wenting Xie. *Cyber behaviors of immigrants*. Encyclopedia of Cyber Behavior, 259-272, 2012.

[86] Alexander Cho. Default publicness: Queer youth of color, social media, and being outed by the machine. *New Media & Society*, 20(9):3183–3200, 2018.

[87] Taejoong Chung, David Choffnes, and Alan Mislove. Tunneling for transparency: A large-scale analysis of end-to-end violations in the Internet. In *16th ACM Internet Measurement Conference (IMC)*, 2016.

[88] Citizen Lab. Block test list. `https://github.com/citizenlab/test-lists`.

[89] Danielle Keats Citron. Cyber civil rights. *Boston University Law Review*, 89(1):61–126, February 2009.

[90] Danielle Keats Citron and Daniel J. Solove. Privacy harms. *SSRN Electronic Journal*, 2021.

[91] Richard Clayton, Steven J. Murdoch, and Robert N. M. Watson. Ignoring the Great Firewall of China. In *Privacy Enhancing Technologies Symposium (PETS)*. Springer, 2006.

[92] Cloudflare. `https://www.cloudflare.com`.

[93] Cloudflare. How do I control IP access to my site?, August 2018. `https://support.cloudflare.com/hc/en-us/articles/217074967-How-do-I-control-IP-access-to-my-site-`.

[94] Camille Cobb and Tadayoshi Kohno. How Public Is My Private Life? In *Proceedings of the 26th International Conference on World Wide Web*, 2017.

[95] Mathew Coleman. The “local” migration state: The site-specific devolution of immigration enforcement in the u.s. south. *Law & Policy*, 34(2):159–190, 2012.

[96] Jessica Colnago, Summer Devlin, Maggie Oates, Chelse Swoopes, Lujo Bauer, Lorrie Cranor, and Nicolas Christin. “It’s not actually that horrible”: Exploring Adoption of Two-Factor Authentication at a University. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 2018.

[97] Federal Trade Commission. National do not call registry, no date. `https://www.donotcall.gov`, accessed 2020-08-27.

[98] Google Account Help Community. How many gmail accounts can a person have? - i assume they all have to be linked to one number?, July 2019. `https://support.google.com/accounts/thread/11008132`, accessed 2020-08-26.

[99] Sunny Consolvo, Patrick Gage Kelley, Tara Matthews, Kurt Thomas, Lee Dunn, and Elie Bursztein. "why wouldn't someone think of democracy as a target?": Security practices & challenges of people involved with U.S. political campaigns. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 1181–1198. USENIX Association, August 2021.

[100] Sasha Constanza-Chock. Digital popular communication lessons on information and communication technologies for social change from the immigrant rights movement national. *Civic Review*, pages 29–35, Fall 2011.

[101] Council of European Union. Council regulation (EU) no A8-0172/2017, 2017.

[102] Joseph Cox. I gave a bounty hunter $300. then he located our phone. Vice, January 2019. Accessed 2020-08-10.

[103] Kimberlé Crenshaw. Demarginalizing the intersection of race and sex: A black feminist critique of antidiscrimination doctrine, feminist theory and antiracist politics. *University of Chicago Legal Forum*, 1989(1):139–167, 1989.

[104] Kimberle Crenshaw. Mapping the margins: Intersectionality, identity politics, and violence against women of color. *Stanford Law Review*, 43(6):1241–1299, 1990.

[105] Stephen M. Croucher. Social networking and cultural adaptation: A theoretical model. *Journal of International and Intercultural Communication*, 4(4):259–264, 2011.

[106] Scott Cunningham and Todd D. Kendall. Prostitution 2.0: The changing face of sex work. *Journal of Urban Economics*, 69(3), 2011.

[107] Paisley Currah and Tara Mulqueen. Securitizing gender: Identity, biometrics, and transgender bodies at the airport. *Social Research*, 78(2):557–582, 2011.

[108] CVS. Pharmacy text alerts, no date. `https://www.cvs.com/mobile-cvs/text`, accessed 2020-08-27.

[109] 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.

[110] 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 *11th ACM Internet Measurement Conference (IMC)*, 2011.

[111] Jakub Dalek, Bennett Haselton, Helmi Noman, Adam Senft, Masashi Crete-Nishihata, Phillipa Gill, and Ronald J. Deibert. A method for identifying and confirming the use of URL filtering products for censorship. In *14th ACM Internet Measurement Conference (IMC)*, 2014.

[112] Avery P Dame-Griff. Trans cultures online. *The International Encyclopedia of Gender, Media, and Communication*, 2020.

[113] Ralf De Wolf, Koen Willaert, and Jo Pierson. Managing privacy boundaries together: Exploring individual and group privacy management strategies in facebook. *Computers in Human Behavior*, 35:444–454, 2014.

[114] Richard Delgado, Jean Stefancic, and Ernesto Liendo. *Critical Race Theory: An Introduction, Second Edition*. New York University Press, 2012.

[115] Department of Homeland Security. Exercising prosecutorial discretion wiht respect to individuals who came to the united states as children, June 2012. [Online; Retrieved 17 September 2017].

[116] U.S. Department of the Treasury. Office of Foreign Assets Control (OFAC). `https://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Foreign-Assets-Control.aspx`.

[117] Bundesrepublik Deutschland. Telemediengesetz (tmg). `https://www.gesetze-im-internet.de/tmg/__5.html`, accessed 2020-10-12.

[118] Diaspora, 2017. `https://diasporafoundation.org/`.

[119] E.J. Dickson. Airbnb: Who's allowed to use the popular home-sharing site? Rolling Stone, January 2020. `https://www.rollingstone.com/culture/culture-news/airbnb-sex-worker-discrimination-935048/`, accessed 2022-04-04.

[120] Roger Dingledine, Nick Mathewson, and Paul Syverson. Tor: The second-generation onion router. In *Proceedings of the 13th USENIX Security Symposium*. USENIX, 2004.

[121] Pranav Dixit. People Are Really Mad About Facebook's Changes To WhatsApp's Privacy Policies. Buzzfeed News, January 2021. `https://www.buzzfeednews.com/article/pranavdixit/whatsapp-privacy-policy-changes`, accessed 2021-02-21.

[122] Periwinkle Doerfler, Kurt Thomas, Maija Marincenko, Juri Ranieri, Yu Jiang, Angelika Moscicki, and Damon McCoy. Evaluating login challenges as a defense against account takeover. In *The World Wide Web Conference*, WWW '19, pages 372–382, New York, NY, USA, 2019. Association for Computing Machinery.

[123] James Doubek. What happens when you get sir mix-a-lot's phone number. NPR, January 2016. `https://www.npr.org/2016/01/16/463219936/what-happens-when-you-get-sir-mix-a-lots-phone-number`, accessed 2020-08-27.

[124] Nora A Draper and Joseph Turow. The corporate cultivation of digital resignation. *New Media & Society*, 21(8):1824–1839, 2019.

[125] Maeve Duggan. Online harassment 2017. Technical report, Pew Research Center, July 2017.

[126] Stefanie Duguay. "he has a way gayer facebook than i do": Investigating sexual identity disclosure and context collapse on a social networking site. *New Media & Society*, 18(6):891–907, 2016.

[127] Zakir Durumeric, David Adrian, Ariana Mirian, Michael Bailey, and J Alex Halderman. A search engine backed by Internet-wide scanning. In *22nd ACM Conference on Computer and Communications Security (CCS)*, pages 542–553, 2015.

[128] J. Dutson, D. Allen, D. Eggett, and K. Seamons. Don't punish all of us: Measuring user attitudes about two-factor authentication. In *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS PW)*, 2019.

[129] Nicole B. Ellison, Charles Steinfield, and Cliff Lampe. Connection strategies: Social capital implications of facebook-enabled communication practices. *New Media & Society*, 13(6):873–892, 2011.

[130] Laura E. Enriquez. 'because we feel the pressure and we also feel the support': Examining the educational success of undocumented immigrant latina/o students. *Harvard Educational Review*, 81(3):476–500, 2011.

[131] Sheena Erete, Yolanda A Rankin, and Jakita O Thomas. I can't breathe: Reflections from black women in cscw and hci. *Proceedings of the ACM on Human-Computer Interaction*, 4(CSCW3):234:1–234:23, 2021.

[132] Facebook. Content restrictions based on local law, 2017. `https://transparency.facebook.com/content-restrictions`.

[133] Facebook. Custom audiences from your customer list, no date. `https://www.facebook.com/business/help/170456843145568?id=2469097953376494&helpref=search&sr=5&query=custom%20audience`, accessed 2021-01-12.

[134] Facebook. Facebook community standards (iv)(18) misrepresentation, no date. `https://www.facebook.com/communitystandards/misrepresentation`, accessed 2020-08-27.

[135] Facebook. How does facebook use my mobile phone number?, no date. `https://www.facebook.com/help/251747795694485`, accessed 2020-08-26.

[136] Facebook. I'm receiving email or text notifications about a facebook account that doesn't belong to me., no date. `https://www.facebook.com/help/225089214296643/?ref=u2u`, accessed 2020-09-01.

[137] Facebook. Where do people you may know suggestions come from?, no date. `https://www.facebook.com/help/163810437015615`, accessed 2020-08-10.

[138] Valerie Fanelle, Sepideh Karimi, Aditi Shah, Bharath Subramanian, and Sauvik Das. Blind and human: Exploring more usable audio CAPTCHA designs. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*, pages 111–125. USENIX Association, August 2020.

[139] FCC. Second report and order, December 2018. `https://docs.fcc.gov/public/attachments/FCC-18-177A1.pdf`, accessed 2020-08-10.

[140] Valerie Feldman. Sex Work Politics and the Internet. In Carisa R. Showden and Samantha Majic, editors, *Negotiating Sex Work*, chapter 11. University of Minnesota Press, 2014.

[141] Adrienne Porter Felt, Richard Barnes, April King, Chris Palmer, Chris Bentzel, and Parisa Tabriz. Measuring HTTPS adoption on the web. In *26th USENIX Security Symposium (USENIX Security 17)*, pages 1323–1338, Vancouver, BC, August 2017. USENIX Association.

[142] R. Fielding and J. Reschke. Hypertext transfer protocol (HTTP/1.1): Semantics and content, June 2014.

[143] Arturo Filastò and Jacob Appelbaum. OONI: Open Observatory of Network Interference. In *2nd USENIX Workshop on Free and Open Communications on the Internet (FOCI)*, 2012.

[144] Juniper Fitzgerald and Jessie Sage. Shadowbans: Secret policies depriving sex workers of income and community. Tits and Sass, June 2019. `https://titsandsass.com/shadowbans-secret-policies-depriving-sex-workers-of-income-and-community/`, accessed 2022-04-05.

[145] Paul J. Fleming, William D. Lopez, Hannah Mesa, Raymond Rion, Ellen Rabinowitz, Richard Bryce, and Monika Doshi. A qualitative study on the impact of the 2016 us election on the health of immigrant families in southeast michigan. *BMC Public Health*, 19(1):947, Jul 2019.

[146] Dinei Florencio and Cormac Herley. A large-scale study of web password habits. In *Proceedings of the 16th International Conference on World Wide Web*, WWW '07, pages 657–666, New York, NY, USA, 2007. Association for Computing Machinery.

[147] Adolfo Flores. People are worried about dhs plans to gather social media info. *Buzzfeed News*, September 2017. [Online; Retrieved 17 September 2017].

[148] Welcoming Center for New Pennsylvanians. *Digital Diaspora: How Immigrants Are Capitalizing on Today's Technology*. Welcoming Center for New Pennsylvanians, Philadelphia, 2012.

[149] Forbes On Marketing. Social media and the big data explosion, Jul 2012.

[150] Adrian Harris Forman. My phone number's other woman. The New York Times, October 2012. https://www.nytimes.com/2012/10/14/opinion/sunday/my-phone-numbers-other-woman.html, accessed 2020-08-27.

[151] Antigoni-Maria Founta, Constantinos Djouvas, Despoina Chatzakou, Ilias Leontiadis, Jeremy Blackburn, Gianluca Stringhini, Athena Vakali, Michael Sirivianos, and Nicolas Kourtellis. Large scale crowdsourcing and characterization of twitter abusive behavior. *arXiv preprint arXiv:1802.00393*, 2018.

[152] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. "a stalker's paradise": How intimate partner abusers exploit technology. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 2018.

[153] Freedom House. Freedom on the net 2016, November 2016.

[154] Alisa Frik, Leysan Nurgalieva, Julia Bernd, Joyce Lee, Florian Schaub, and Serge Egelman. Privacy and security threat models and mitigation strategies of older adults. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, pages 21–40, Santa Clara, CA, August 2019. USENIX Association.

[155] McKenzie Funk. How ice picks its targets in the surveillance age. The New York Times, October 2019. https://www.nytimes.com/2019/10/02/magazine/ice-surveillance-deportation.html, accessed 2021-04-28.

[156] Kevin Gallagher, Sameer Patil, and Nasir Memon. New me: Understanding expert and non-expert perceptions and usage of the tor anonymity network. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, 2017.

[157] Simson Garfinkel and Heather Richter Lipford. Usable security: History, themes, and challenges. *Synthesis Lectures on Information Security, Privacy, and Trust*, 5(2):1–124, 2014.

[158] Christine Geeng and Alexis Hiniker. Lgbtq privacy concerns on social media. In *Moving Beyond a 'One-size-fits-all' approach: exploring individual differences in privacy*, CHI Workshop, New York, NY, USA, 2018. Association for Computing Machinery.

[159] Christine Geeng, Jevan Hutson, and Franziska Roesner. Usable sexurity: Studying People's concerns and strategies when sexting. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*, pages 127–144. USENIX Association, August 2020.

[160] Maximilian Golla, Miranda Wei, Juliette Hainline, Lydia Filipe, Markus Dürmuth, Elissa Redmiles, and Blase Ur. "what was that site doing with my facebook password?": Designing password-reuse notifications. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, CCS '18, pages 1549–1566, New York, NY, USA, 2018. Association for Computing Machinery.

[161] Ruth Gomberg-Muñoz. *Labor and Legality: An Ethnography of a Mexican Immigrant Network*. Oxford University Press, New York, 2011.

[162] Ricardo Gomez and Sara Vannini. *Fotohistorias: Participatory Photography and the Experience of Migration*. CreateSpace Independent Publishing Platform, Seattle, WA., 2015.

[163] Roberto G. Gonzales and Leo R. Chavez. "awakening to a nightmare": Abjectivity and illegality in the lives of undocumented 1.5-generation latino immigrants in the united states. *Current Anthropology*, 53(3):255–281, 2012.

[164] Roberto. G. Gonzales and Steven Raphael. Illegality: A contemporary portrait of immigration. *RSF: The Russell Sage Foundation Journal of the Social Sciences*, 3(4):1–17, 2017.

[165] Lauren Goode. I called off my wedding. the internet will never forget. Wired, April 2021. `https://www.wired.com/story/weddings-social-media-apps-photos-memories-miscarriage-problem/`, last accessed 2022-04-04.

[166] Google. Countries or regions with restricted access. `https://support.google.com/a/answer/2891389`.

[167] Google. Google appengine faq. `https://cloud.google.com/appengine/kb/#static-ip`.

[168] Google. How to use dual sims on your google pixel phone, no date. `https://support.google.com/pixelphone/answer/9449293`, accessed 2020-08-12.

[169] Google. Set up a recovery phone number or email address, no date. `https://support.google.com/accounts/answer/183723`, accessed 2020-08-26.

[170] Google. Sign in with your phone instead of a password, no date. `https://support.google.com/accounts/answer/6361026`, accessed 2020-08-27.

[171] Google. Verify your account, no date. `https://support.google.com/accounts/answer/114129`, accessed 2020-08-25.

[172] Paul A. Grassi, James L. Fenton, Elaine M. Newton, Ray A. Perlner, Andrew R. Regenscheid, William E. Burr, Justin P. Richer, Naomi B. Lefkovitz, Jamie M. Danker, Yee-Yin Choong, Kristen K. Greene, and Mary F. Theofanos. Digital identity guidelines: Authentication and lifecycle management, 3 2019. NIST Special Publication 800-63B.

[173] Colin M. Gray, Yubo Kou, Bryan Battles, Joseph Hoggatt, and Austin L. Toombs. The dark (patterns) side of ux design. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, CHI '18, page 1–14, New York, NY, USA, 2018. Association for Computing Machinery.

[174] GreatFire.org. https://en.greatfire.org.

[175] Glenn Greenwald. *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. Metropolitan Books, 2014.

[176] Roger Grimes. The many ways to hack 2FA. *Network Security*, 2019(9):8–13, 2019.

[177] Ralph Gross and Alessandro Acquisti. Information revelation and privacy in online social networks. In *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*, WPES '05, pages 71–80, New York, NY, USA, 2005. ACM.

[178] World Bank Group. Digital identity: Towards shared principles for public and private sector cooperation, July 2016. http://documents.worldbank.org/curated/en/600821469220400272/pdf/107201-WP-PUBLIC-WB-GSMA-SIADigitalIdentity-WEB.pdf, accessed 2020-08-27.

[179] 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 *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, CHI '18, New York, NY, USA, 2018. Association for Computing Machinery.

[180] Lauren E. Gulbas and Luis H. Zayas. Exploring the effects of u.s immigration enforcement on the well-being of citizen children in mexican immigrant families. *RSF: The Russell Sage Foundation Journal of the Social Sciences*, 3(4):53–69, 2017.

[181] Hacking//Hustling. About hacking//hustling. https://hackinghustling.org, accessed on 2021-02-19.

[182] Oliver L. Haimson, Jed R. Brubaker, Lynn Dombrowski, and Gillian R. Hayes. Digital footprints and changing networks during online identity transitions. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, CHI '16, page 2895–2907, New York, NY, USA, 2016. Association for Computing Machinery.

[183] Oliver L Haimson, Avery Dame-Griff, Elias Capello, and Zahari Richter. Tumblr was a trans technology: the meaning, importance, history, and future of trans technologies. *Feminist Media Studies*, 2019.

[184] Foad Hamidi, Morgan Klaus Scheuerman, and Stacy M. Branham. Gender recognition or gender reductionism? the social implications of embedded gender recognition systems. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, CHI '18, page 1–13, New York, NY, USA, 2018. Association for Computing Machinery.

[185] Lisa J Hardy, Christina M Getrich, Julio C Quezada, Amanda Guay, Raymond J Michalowski, and Eric Henley. A call for further research on the impact of state-level immigration policies on public health. *American journal of public health*, 102(7):1250–1253, 2012.

[186] Eszter Hargittai and Alice Marwick. “what can i really do?” explaining the privacy paradox with online apathy. *International Journal of Communication*, 10:3737–3757, 2016.

[187] Sam Havron, Diana Freed, Rahul Chatterjee, Damon McCoy, Nicola Dell, and Thomas Ristenpart. Clinical computer security for victims of intimate partner violence. In *28th USENIX Security Symposium (USENIX Security 19)*, 2019.

[188] Jordan Hayes, Smirity Kaushik, Charlotte Emily Price, and Yang Wang. Cooperative privacy and security: Learning from people with visual impairments and their allies. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, pages 1–20, Santa Clara, CA, August 2019. USENIX Association.

[189] Cormac Herley. So long, and no thanks for the externalities: the rational rejection of security advice by users. In *Proceedings of the 2009 workshop on New security paradigms workshop*, 2009.

[190] Kashmir Hill. How facebook outs sex workers. Gizmodo, October 2017. https://gizmodo.com/how-facebook-outs-sex-workers-1818861596, accessed 2020-09-01.

[191] Kashmir Hill. Wrongfully accused by an algorithm. The New York Times, June 2020. , accessed 2022-04-13.

[192] Hiya. Mr number: Call block & reverse lookup, no date. https://hiya.com/downloads, accessed 2020-08-27.

[193] Bernie Hogan. The presentation of self in the age of social media: Distinguishing performances and exhibitions online. *Bulletin of Science, Technology & Society*, 30(6):377–386, 2010.

[194] Hola unblocker. https://hola.org.

[195] Avery E. Holton, Valérie Bélair-Gagnon, Diana Bossio, and Logan Molyneux. “not their fault, but their problem”: Organizational responses to the online harassment of journalists. *Journalism Practice*, 0(0):1–16, 2021.

[196] Karen Holtzblatt, Jessamyn Burns Wendell, and Shelley Wood. *Rapid contextual design: a how-to guide to key techniques for user-centered design*. The Morgan Kaufmann series in interactive technologies. Elsevier/Morgan Kaufmann, 2005.

[197] Shan Huang, Félix Cuadrado, and Steve Uhlig. Middleboxes in the Internet: a HTTP perspective. In *Network Traffic Measurement and Analysis Conference (TMA)*, pages 1–9. IEEE, 2017.

[198] Damilola Ibosiola, Ignacio Castro, Gianluca Stringhini, Steve Uhlig, and Gareth Tyson. Who watches the watchmen: Exploring complaints on the web. In *The World Wide Web Conference*, 2019.

[199] Samia Ibtasam, Lubna Razaq, Maryam Ayub, Jennifer R. Webster, Syed Ishtiaque Ahmed, and Richard Anderson. "my cousin bought the phone for me. i never go to mobile shops.": The role of family in women's technological inclusion in islamic culture. *Proc. ACM Hum.-Comput. Interact.*, 3(CSCW), nov 2019.

[200] Sarah E. Igo. *The Known Citizen*. Harvard University Press, USA, 2018.

[201] 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 *16th ACM Internet Measurement Conference (IMC)*, pages 349–364, 2016.

[202] International Monetary Fund. World economic outlook database. `http://www.imf.org/external/pubs/ft/weo/2014/02/weodata/index.aspx`.

[203] Iulia Ion, Rob Reeder, and Sunny Consolvo. "...no one can hack my mind": Comparing expert and non-expert security practices. *In Proc. Symposium on Usable Privacy and Security (SOUPS'15), USENIX*, 2015.

[204] Andrew Henry Jakubowicz. Alt_right white lite: trolling, hate speech and cyber racism on social media. *Cosmopolitan Civil Societies: an Interdisciplinary Journal*, 9(3):41–60, 2017.

[205] Sandy E. James, Jody L Herman, Susan Rankin, Mara Keisling, LIsa Mottet, and Ma'ayan Anafi. The Report of the 2015 U.S. Transgender Survey. Technical report, National Center for Transgender Equality, 2016.

[206] Alison Grace Johansen. 5 kinds of id theft using a social security number. NortonLifeLock, no date. `https://www.lifelock.com/learn-identity-theft-resources-kinds-of-id-theft-using-social-security-number.html`, accessed 2020-08-15.

[207] Lisa Grazina Johnston, Keith Sabin, Mai Thu Hien, and Pham Thi Huong. Assessment of respondent driven sampling for recruiting female sex workers in two vietnamese cities: reaching the unseen sex worker. *Journal of Urban Health*, 83(1), 2006.

[208] Angela Jones. Sex Work in a Digital Era. *Sociology Compass*, 9(7), 2015.

[209] Angela Jones. "I get paid to have orgasms": Adult webcam models' negotiation of pleasure and danger. *Signs*, 42(1), 2016.

[210] Angela Jones. *Camming*. NYU Press, 2020.

[211] Ben Jones, Tzu-Wen Lee, Nick Feamster, and Phillipa Gill. Automated detection and fingerprinting of censorship block pages. In *14th ACM Internet Measurement Conference (IMC)*, 2014.

[212] Michael Jones-Correa and James A. McCann. In the public but not the electorate: The "civic status gap" in the united states. *RSF: The Russell Sage Foundation Journal of the Social Sciences*, 2(3):1–19, 2016.

[213] jp88. Phone number limit. Google Account Help Community, September 2019. https://support.google.com/accounts/thread/13443342, accessed 2020-08-23.

[214] Anil Kalhan. Immigration policing and federalism through the lens of technology, surveillance and privacy. *Ohio State Law Journal*, 74, 2013.

[215] Sara Kamali. Informants, provocateurs, and entrapment: Examining the histories of the fbi's patcon and the nypd's muslim surveillance program. *Surveillance & Society*, 15(1), Feb 2017.

[216] Seny Kamara. Crypto for the people, 2020. https://www.youtube.com/watch?v=Ygq9ci0GFhA, accessed 2020-10-15.

[217] 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, Ottawa, 2015. USENIX Association.

[218] Os Keyes. The misgendering machines: Trans/hci implications of automatic gender recognition. *Proc. ACM Hum.-Comput. Interact.*, 2(CSCW), nov 2018.

[219] Sheharbano Khattak, Tariq Elahi, Laurent Simon, Colleen M Swanson, Steven J Murdoch, and Ian Goldberg. SOK: Making sense of censorship resistance systems. *Proceedings on Privacy Enhancing Technologies*, 2016(4):37–61, 2016.

[220] Sheharbano Khattak, Mobin Javed, Syed Ali Khayam, Zartash Afzal Uzmi, and Vern Paxson. A look at the consequences of Internet censorship through an ISP lens. In *14th ACM Internet Measurement Conference (IMC)*, pages 271–284, 2014.

[221] Walter Kirn. If you're not paranoid, you're crazy. The Atlantic, November 2015. https://www.theatlantic.com/magazine/archive/2015/11/if-youre-not-paranoid-youre-crazy/407833, accessed 2020-08-10.

[222] Amy J. Ko. 100 hours of name change labor, 2019.

[223] Richie Koch. The proton guide to privacy at protests, 2020. https://protonmail.com/blog/how-to-protect-privacy-at-protests/, accessed 2020-09-11.

[224] Saranga Komanduri, Richard Shay, Patrick Gage Kelley, Michelle L. Mazurek, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, and Serge Egelman. Of passwords and people: Measuring the effect of password-composition policies. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '11, pages 2595–2604, New York, NY, USA, 2011. ACM.

[225] Jess Kropczynski, Zaina Aljallad, Nathan Jeffrey Elrod, Heather Lipford, and Pamela J. Wisniewski. Towards building community collective efficacy for managing digital privacy and security within older adult communities. *Proc. ACM Hum.-Comput. Interact.*, 4(CSCW3), jan 2021.

[226] Priya Kumar, Shalmali Milind Naik, Utkarsha Ramesh Devkar, Marshini Chetty, Tamara L. Clegg, and Jessica Vitak. 'no telling passcodes out because they're private': Understanding children's mental models of privacy and security online. *Proc. ACM Hum.-Comput. Interact.*, 1(CSCW), dec 2017.

[227] Pawel Laka and Wojciech Mazurczyk. User perspective and security of a new mobile authentication method. *Telecommunication Systems*, 69(3):365–379, Nov 2018.

[228] Ravie Lakshmanan. Loyalty programs cost you your personal data - are the rewards worth it? The Next Web, June 2019. `https://thenextweb.com/insights/2019/06/12/loyalty-programs-cost-you-your-personal-data-are-the-rewards-worth-it/`, accessed 2020-09-01.

[229] Airi Lampinen, Vilma Lehtinen, Asko Lehmuskallio, and Sakari Tamminen. We're in it together: Interpersonal management of disclosure in social network services. *In Proc. SIGCHI Conference on Human Factors in Computing Systems (CHI '11) ACM*, pages 3217–3226, 2011.

[230] Selena Larson. Every single yahoo account was hacked - 3 billion in all, 2020. `https://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/index.html`, accessed 2020-09-11.

[231] Stevens Le Blond, Alejandro Cuevas, Juan Ramón Troncoso-Pastoriza, Philipp Jovanovic, Bryan Ford, and Jean-Pierre Hubaux. On enforcing the digital immunity of a large humanitarian organization. In *2018 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2018.

[232] Kevin Lee, Benjamin Kaiser, Jonathan Mayer, and Arvind Narayanan. An empirical study of wireless carrier authentication for SIM swaps. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*, pages 61–79, USA, 2020. USENIX.

[233] Roxanne Leitão. Anticipating smart home security and privacy threats with survivors of intimate partner abuse. In *Proceedings of the 2019 on Designing Interactive Systems Conference*, DIS '19, page 527–539, New York, NY, USA, 2019. Association for Computing Machinery.

[234] Ada Lerner, Helen Yuxun He, Anna Kawakami, Silvia Catherine Zeamer, and Roberto Hoyle. *Privacy and Activism in the Transgender Community*, page 1–13. Association for Computing Machinery, New York, NY, USA, 2020.

[235] Jialiu Lin, Shahriyar Amini, Jason I. Hong, Norman Sadeh, Janne Lindqvist, and Joy Zhang. Expectation and purpose: Understanding users' mental models of mobile app privacy through crowdsourcing. In *Proceedings of the 2012 ACM Conference on*

Ubiquitous Computing, UbiComp '12, pages 501–510, New York, NY, USA, 2012. ACM.

[236] Dara Lind. Fewer immigrants are being deported under trump than under obama: But it's not because trump isn't trying. *Vox*, Aug. 2017. [Online; Retrieved 17 September 2017].

[237] Eden Litt and Eszter Hargittai. A bumpy ride on the information superhighway: Exploring turbulence online. *Computers in Human Behavior*, 36:520–529, 2014.

[238] Yabing Liu, Krishna P. Gummadi, Balachander Krishnamurthy, and Alan Mislove. Analyzing facebook privacy settings: user expectations vs. reality. In *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference*, IMC '11, page 61–70. Association for Computing Machinery, Nov 2011.

[239] Dana Lone Hill. Facebook don't believe in indian names. Last Real Indians, February 2015. `https://lastrealindians.com/news/2015/2/6/feb-6-2015-facebook-dont-believe-in-indian-names-by-dana-lone-hill`.

[240] William D Lopez, Daniel J Kruger, Jorge Delva, Mikel Llanes, Charo Ledón, Adreanne Waller, Melanie Harner, Ramiro Martinez, Laura Sanders, Margaret Harner, et al. Health implications of an immigration raid: findings from a latino community in the midwestern united states. *Journal of immigrant and minority health*, 19(3):702–708, 2017.

[241] Graham Lowe, Patrick Winters, and Michael L Marcus. The great DNS wall of China. *MS, New York University*, 21, 2007.

[242] Gus Lubin. There are 42 million prostitutes in the world, and here's where they live. Business Insider, 2012. `https://www.businessinsider.com/there-are-42-million-prostitutes-in-the-world-and-heres-where-they-live-2012-1`, accessed 2020-09-16.

[243] Luminati. `https://luminati.io`.

[244] Mary Madden. Privacy, security, and digital inequality. Research report, Data & Society, 2017.

[245] 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 (USENIX Security 14)*, pages 511–525, San Diego, CA, August 2014. USENIX Association.

[246] Alice E. Marwick and danah boyd. I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience. *New Media and Society*, 13(1), 2011.

[247] Alice E. Marwick and danah boyd. Privacy at the margins| understanding privacy at the margins—introduction. *International Journal of Communication*, 12(00):9, Mar 2018.

[248] Mastodon. Decentralized social network, 2017. `https://mastodon.social`.

[249] 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*, 2017.

[250] Roger C Mayer, James H Davis, and F David Schoorman. An integrative model of organizational trust. *Academy of management review*, 20(3):709–734, 1995.

[251] 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.

[252] Allison McDonald, Matthew Bernhard, Luke Valenta, Benjamin VanderSloot, Will Scott, Nick Sullivan, J. Alex Halderman, and Roya Ensafi. 403 forbidden: A global view of cdn geoblocking. In *Proceedings of the Internet Measurement Conference 2018*, 2018.

[253] Allison McDonald, Carlo Sugatan, Tamy Guberek, and Florian Schaub. The annoying, the disturbing, and the weird: Challenges with phone numbers as identifiers and phone number recycling. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, CHI '21, New York, NY, USA, 2021. Association for Computing Machinery.

[254] Nora McDonald and Andrea Forte. The politics of privacy theories: Moving from norms to vulnerabilities. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, page 1–14. ACM, Apr 2020.

[255] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. Reliability and inter-rater reliability in qualitative research: Norms and guidelines for cscw and hci practice. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW), 2019.

[256] Susan McGregor, Franziska Roesner, and Kelly Caine. Individual versus organizational computer security and privacy concerns in journalism. *Proc. Privacy Enhancing Technologies*, 4, 2016.

[257] Susan E. McGregor, Polina Charters, Tobin Holliday, and Franziska Roesner. Investigating the computer security practices and needs of journalists. In *24th USENIX Security Symposium (USENIX Security 15)*, 2015.

[258] Mary L. McHugh. Interrater reliability: The kappa statistic. *Biochemia Medica*, 22:276–282, 2012.

[259] William Melicher, Darya Kurilova, Sean M. Segreti, Pranshu Kalvani, Richard Shay, Blase Ur, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, and Michelle L. Mazurek. Usability and security of text passwords on mobile devices. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, CHI '16, pages 527–539, New York, NY, USA, 2016. ACM.

[260] Cecilia Menjívar. Liminal legality: Salvadoran and guatemalan immigrants' lives in the united states. *American Journal of Sociology*, 111(4):999–1037, 2006.

[261] Helena M. Mentis, Galina Madjaroff, Aaron Massey, and Zoya Trendafilova. The illusion of choice in discussing cybersecurity safeguards between older adults with mild cognitive impairment and their caregivers. *Proc. ACM Hum.-Comput. Interact.*, 4(CSCW2), oct 2020.

[262] M Giovanna Merli, James Moody, Jeffrey Smith, Jing Li, Sharon Weir, and Xiangsheng Chen. Challenges to recruiting population representative samples of female sex workers in china using respondent driven sampling. *Social Science & Medicine*, 125, 2015.

[263] Lil Miss Hot Mess. Selfies and side-eye: Drag queens take on facebook. *Studies in Gender and Sexuality*, 16(2):144–146, 2015.

[264] Mijente, Immigrant Defense Project, and the National Immigration Project of the National Lawyers Guild. Who's behind ice? the tech companies fueling deportations, 2018. `https://mijente.net/wp-content/uploads/2018/10/WHO%E2%80%99S-BEHIND-ICE_-The-Tech-and-Data-Companies-Fueling-Deportations-_v1.pdf`, accessed 2022-04-05.

[265] Matthew B Miles, A Michael Huberman, and Johnny Saldaña. Qualitative data analysis: A methods sourcebook. 3rd, 2014.

[266] Ariana Mirian, Joe DeBlasio, Stefan Savage, Geoffrey M. Voelker, and Kurt Thomas. Hack for hire: Exploring the emerging market for account hijacking. In *The World Wide Web Conference*, WWW '19, pages 1279–1289, New York, NY, USA, 2019. Association for Computing Machinery.

[267] David Moher, Alessandro Liberati, Jennifer Tetzlaff, and Douglas G. Altman. Preferred reporting items for systematic reviews and meta-analyses: The prisma statement. *Journal of Clinical Epidemiology*, 62(10):1006–1012, Oct 2009.

[268] Jessica D. Moorman and Kristen Harrison. Gender, Race, and Risk: Intersectional Risk Management in the Sale of Sex Online. *Journal of Sex Research*, 53(7), 2016.

[269] National Ugly Mugs. National ugly mugs. `https://uglymugs.org`, accessed 2020-10-04.

[270] Savanthi Murthy, Karthik S. Bhat, Sauvik Das, and Neha Kumar. Individually vulnerable, collectively safe: The security and privacy practices of households with older adults. *Proc. ACM Hum.-Comput. Interact.*, 5(CSCW1), apr 2021.

[271] Ana Muñiz. Secondary ensnarement: Surveillance systems in the service of punitive immigration enforcement. *Punishment & Society*, 22(4):461–482, Oct 2020.

[272] Zubair Nabi. The anatomy of Web censorship in Pakistan. In *1st USENIX Workshop on Free and Open Communications on the Internet (FOCI)*, 2013.

[273] Brian Naylor. Trump's plan to hire 15,000 border patrol and ice agents won't be easy, February 2017. [Online; Retrieved 17 September 2017].

[274] New York Times. Google, seeking a return to china, is said to be building a censored search engine, August 2018. `https://www.nytimes.com/2018/08/01/technology/china-google-censored-search-engine.html`.

[275] Lily Hay Newman. Phone numbers were never meant as id. now we're all at risk. Wired, August 2018. `https://www.wired.com/story/phone-numbers-indentification-authentication`, accessed 2020-08-26.

[276] Nathan Newman. The costs of lost privacy: Consumer harm and rising economic inequality in the age of google. *William Mitchell Law Review*, 40(2), 2014.

[277] Casey Newton. Inside twitter's ambitious plan to kill the password. The Verge, October 2014. `https://www.theverge.com/2014/10/22/7034113/inside-twitters-ambitious-plan-to-kill-the-password-on-mobile-devices`, accessed 2020-08-27.

[278] Laura Nichols. Social desire paths: a new theoretical concept to increase the usability of social science research in society. *Theory and Society*, 43(6):647–665, Nov 2014.

[279] Helen Nissenbaum. *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press, 2009.

[280] Safiya Umoja Noble. *Algorithms of Oppression*. NYU Press, 2018.

[281] Patricia A. Norberg, Daniel R. Horne, and David A. Horne. The privacy paradox: Personal information disclosure intentions versus behaviors. *J Consumer Affairs*, 41(1):100–126, 2007.

[282] Fayika Farhat Nova, Michael Ann DeVito, Pratyasha Saha, Kazi Shohanur Rashid, Shashwata Roy Turzo, Sadia Afrin, and Shion Guha. *Understanding How Marginalized Hijra in Bangladesh Navigate Complex Social Media Ecosystem*, page 353–358. Association for Computing Machinery, New York, NY, USA, 2020.

[283] Nicole Novak, Arline T. Geronimus, and Aresha M. Martinez-Cardoso. Change in birth outcomes among infants born to latina mothers after a major immigration raid. *International Journal of Epidemiology*, 46(3):839–849, 1 June 2017.

[284] Borke Obada-Obieh, Lucrezia Spagnolo, and Konstantin Beznosov. Towards understanding privacy and trust in online reporting of sexual assault. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*, pages 145–164. USENIX Association, August 2020.

[285] Ziad Obermeyer, Brian Powers, Christine Vogeli, and Sendhil Mullainathan. Dissecting racial bias in an algorithm used to manage the health of populations. *Science*, 366(6464):447–453, 2019.

[286] Ihudiya Finda Ogbonnaya-Ogburu, Angela D.R. Smith, Alexandra To, and Kentaro Toyama. *Critical Race Theory for HCI*, page 1–16. Association for Computing Machinery, New York, NY, USA, 2020.

[287] Ihudiya Finda Ogbonnaya-Ogburu, Kentaro Toyama, and Tawanna R. Dillahunt. Towards an effective digital literacy intervention to assist returning citizens with job search. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, CHI '19, page 1–12, New York, NY, USA, 2019. Association for Computing Machinery.

[288] Michael A. Olivas. Immigration-related state and local ordinances: Preemption, prejudice, and the proper role for enforcement. *University of Chicago Legal Forum*, 2007(1), 2007.

[289] Joint United Nations Programme on HIV/AIDS (UNAIDS), Data UNAIDS, et al. Geneva, Switzerland; 2018. *North American, Western and Central Europe: AIDS epidemic update regional summary*, 2019.

[290] OpenNet Initiative. Survey of government Internet filtering practices indicates increasing internet censorship, May 2007. `https://cyber.harvard.edu/newsroom/first_global_filtering_survey_released`.

[291] Kentrell Owens, Camille Cobb, and Lorrie Cranor. "you gotta watch what you say": Surveillance of communication with incarcerated people. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, CHI '21, New York, NY, USA, 2021. Association for Computing Machinery.

[292] Matthew J. Page, Joanne E. McKenzie, Patrick M. Bossuyt, Isabelle Boutron, Tammy C. Hoffmann, Cynthia D. Mulrow, Larissa Shamseer, Jennifer M. Tetzlaff, Elie A. Akl, Sue E. Brennan, and et al. The prisma 2020 statement: an updated guideline for reporting systematic reviews. *BMJ*, 372:n71, Mar 2021.

[293] Leysia Palen and Paul Dourish. Unpacking "privacy" for a networked world. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '03, pages 129–136, New York, NY, USA, 2003. ACM.

[294] Jong Chun Park and Jedidiah R Crandall. Empirical study of a national-scale distributed intrusion detection system: Backbone-level filtering of HTML responses in china. In *International Conference on Distributed Computing Systems (ICDCS)*, pages 315–326. IEEE, 2010.

[295] Jeffrey S. Passel and D'Vera Cohn. As mexican share declined, u.s. unauthorized immigrant population fell in 2015 below recession level. Fact Tank, Pew Research Center, 2017. [Online; Retrieved 17 September 2017].

[296] Faiza Patel, Rachel Levinson-Waldman, Raya Koreh, and Sophia DenUyl. Social media monitoring. Brennan Center for Justice, May 2019. https://www.brennancenter.org/our-work/research-reports/social-media-monitoring, accessed 2022-04-05.

[297] Kari Paul. Why it's perfectly legal for airbnb to discriminate against sex workers. Vice, July 2016. https://www.vice.com/en/article/gvzzkx/why-its-perfectly-legal-for-airbnb-to-discriminate-against-sex-workers, accessed 2020-10-07.

[298] Paypal. Paypal acceptable use policy. https://www.paypal.com/de/webapps/mpp/ua/acceptableuse-full?locale.x=en_DE, accessed 2020-10-12.

[299] Paul Pearce, Roya Ensafi, Frank Li, Nick Feamster, and Vern Paxson. Augur: Internet-wide detection of connectivity disruptions. In *38th IEEE Symposium on Security and Privacy*, May 2017.

[300] F. Pedregosa, G. Varoquaux, A. Gramfort, V. Michel, B. Thirion, O. Grisel, M. Blondel, P. Prettenhofer, R. Weiss, V. Dubourg, J. Vanderplas, A. Passos, D. Cournapeau, M. Brucher, M. Perrot, and E. Duchesnay. Scikit-learn: Machine Learning in Python . *Journal of Machine Learning Research*, 12:2825–2830, 2011.

[301] Sandra Petronio. Communication privacy management theory: What do we know about family privacy regulation? *Journal of Family Theory & Review*, 2(3):175–196, 2010.

[302] Chanda Phelan, Cliff Lampe, and Paul Resnick. It's creepy, but it doesn't bother me. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, CHI '16, page 5240–5251, New York, NY, USA, 2016. Association for Computing Machinery.

[303] James Pierce, Sarah Fox, Nick Merrill, and Richmond Wong. Differential vulnerabilities and a diversity of tactics: What toolkits teach us about cybersecurity. *Proceedings of the ACM on Human-Computer Interaction*, 2(CSCW):139:1–139:24, Nov 2018.

[304] Anthony T. Pinter, Morgan Klaus Scheuerman, and Jed R. Brubaker. Entering doors, evading traps: Benefits and risks of visibility during transgender coming outs. *Proc. ACM Hum.-Comput. Interact.*, 4(CSCW3), jan 2021.

[305] Jane Pitcher and Marjan Wijers. The impact of different regulatory models on the labour conditions, safety and welfare of indoor-based sex workers. *Criminology and Criminal Justice*, 14(5), 2014.

[306] Nathaniel Popper. Identity thieves hijack cellphone accounts to go after virtual currency. The New York Times, August 2017. https://www.nytimes.com/2017/08/21/business/dealbook/phone-hack-bitcoin-virtual-currency.html, accessed 2020-08-26.

[307] Alejandro Portes and Rubén G. Rumbaut. *Immigrant America: A Portrait*. Univ. of California Press, 2006.

[308] Henry F. Pringle and Katherine Pringle. Sixty million headaches every year. The Saturday Evening Post, April 1954. `http://www.saturdayeveningpost.com/wp-content/uploads/satevepost/sixty_million_headaches.pdf`, accessed 2020-08-15.

[309] Anabel Quan-Haase and Dennis Ho. Online privacy concerns and privacy protection strategies among older adults in east york, canada. *Journal of the Association for Information Science and Technology*, 71(9):1089–1102, 2020.

[310] Cooper Quintin. Our cellphones aren't safe. The New York Times, December 2018. `https://www.nytimes.com/2018/12/26/opinion/cellphones-security-spying.html`, accessed 2020-08-16.

[311] Hawra Rabaan, Alyson L. Young, and Lynn Dombrowski. Daughters of men: Saudi women's sociotechnical agency practices in addressing domestic abuse. *Proc. ACM Hum.-Comput. Interact.*, 4(CSCW3), jan 2021.

[312] Emilee Rader and Anjali Munasinghe. "wait, do i know this person?": Understanding misdirected email. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, CHI '19, pages 1–13, New York, NY, USA, 2019. Association for Computing Machinery.

[313] Emilee Rader, Rick Wash, and Brandon Brooks. Stories as informal lessons about security. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*, SOUPS '12, New York, NY, USA, 2012. Association for Computing Machinery.

[314] Fanny Ramirez and Jeffrey Lane. Communication privacy management and digital evidence in an intimate partner violence case. *International Journal of Communication*, 13(0), 2019.

[315] Ashwini Rao, Florian Schaub, Norman Sadeh, Alessandro Acquisti, and Ruogu Kang. Expecting the unexpected: Understanding mismatched privacy expectations online. *In Proc. Symposium on Usable Privacy and Security (SOUPS '16)*, 2016.

[316] Hirak Ray, Flynn Wolf, Ravi Kuber, and Adam J. Aviv. "Warn Them" or "Just Block Them"?: Comparing Privacy Concerns of Older and Working Age Adults. *Proceedings on Privacy Enhancing Technologies (PoPETS)*, July 2021.

[317] Elissa M. Redmiles. Behind the red lights: Methods for investigating the digital security and privacy experiences of sex workers. In Eszter Hargittai, editor, *Research Exposed: How Empirical Social Science Gets Done in the Digital Age*, chapter 5. Columbia University Press, 2020.

[318] Elissa M Redmiles, Jessica Bodford, and Lindsay Blackwell. "I just want to feel safe": A diary study of safety perceptions on social media. In *Proceedings of the International AAAI Conference on Web and Social Media*, volume 13, 2019.

[319] Elissa M Redmiles, Michelle L. Mazurek, and John P Dickerson. Dancing pigs or externalities? Measuring the rationality of security decisions. In *Proceedings of the 2018 ACM Conference on Economics and Computation*, 2018.

[320] 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, USA, August 2020. USENIX Association.

[321] Ken Reese, Trevor Smith, Jonathan Dutson, Jonathan Armknecht, Jacob Cameron, and Kent Seamons. A usability study of five two-factor authentication methods. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, Santa Clara, CA, August 2019. USENIX Association.

[322] Rubén G. Rumbaut and Alejandro Portes. *Ethnicities: Children of immigrants in America*. Univ. of California Press, 2001.

[323] Erin M Sales. The biometric revolution: An erosion of the fifth amendment privilege to be free from self-incrimination. *U. Miami L. Rev.*, 69:193, 2014.

[324] J. H. Saltzer and M. Schroeder. The protection of information in computer systems. *Proceedings of the IEEE*, 63:1278–1308, 1975.

[325] Nithya Sambasivan, Amna Batool, Nova Ahmed, Tara Matthews, Kurt Thomas, Laura Sanely Gaytán-Lugo, David Nemer, Elie Bursztein, Elizabeth Churchill, and Sunny Consolvo. "they don't leave us alone anywhere we go": Gender and digital abuse in south asia. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, CHI '19, page 1–14, New York, NY, USA, 2019. Association for Computing Machinery.

[326] Teela Sanders, Laura Connelly, and Laura Jarvis King. On our own terms: The working conditions of internet-based sex workers in the UK. *Sociological Research Online*, 21(4), 2016.

[327] Teela Sanders, Jane Scoular, Rosie Campbell, Jane Pitcher, and Stewart Cunningham. *Internet Sex Work: Beyond the Gaze*. Palgrave Macmillan, 2018.

[328] Morgan Klaus Scheuerman, Stacy M. Branham, and Foad Hamidi. Safe spaces and safe places: Unpacking technology-mediated experiences of safety and harm with transgender people. *Proc. ACM Hum.-Comput. Interact.*, 2(CSCW), nov 2018.

[329] Bruce Schneier. *Data and Goliath: The hidden battles to collect your data and control your world*. WW Norton & Company, 2015.

[330] John T Scholz and Mark Lubell. Trust and taxpaying: Testing the heuristic approach to collective action. *American Journal of Political Science*, pages 398–417, 1998.

[331] Hyunjin Seo, Hannah Britton, Megha Ramaswamy, Darcey Altschwager, Mathew Blomberg, Shola Aromona, Bernard Schuster, Ellie Booton, Marilyn Ault, and Joi Wickliffe. Returning to the digital world: Digital technology use and privacy management of women transitioning from incarceration. *New Media & Society*, 24(3):641–666, 2020.

[332] Diala Shamas and Nermeen Arastu. Mapping muslims: Nypd spying and its impact on american muslims, 2013.

[333] Richard Shay, Iulia Ion, Robert W. Reeder, and Sunny Consolvo. "my religious aunt asked why i was trying to sell her viagra": Experiences with account hijacking. In *Proceedings of the 32Nd Annual ACM Conference on Human Factors in Computing Systems*, CHI '14, pages 2657–2666, New York, NY, USA, 2014. ACM.

[334] Sebastian Shehadi and Miriam Partington. Coronavirus: Offline sex workers forced to start again online. BBC, April 2020. `https://www.bbc.com/news/technology-52183773`.

[335] Fatemeh Shirazi and Melanie Volkamer. What deters jane from preventing identification and tracking on the web? In *Proceedings of the 13th Workshop on Privacy in the Electronic Society*, WPES '14, pages 107–116, New York, NY, USA, 2014. ACM.

[336] Hossein Siadati, Toan Nguyen, Payas Gupta, Markus Jakobsson, and Nasir Memon. Mind your SMSes: Mitigating social engineering in second factor authentication. *Computers and Security*, 65:14–28, 2017.

[337] Dawinder Sidhu. The chilling effect of government surveillance programs on the use of the internet by muslim-americans (june 27, 2011). *University of Maryland Law Journal of Race, Religion, Gender and Class*, 7:375, 2007.

[338] Signal. Register a phone number, no date. `https://support.signal.org/hc/en-us/articles/360007318691-Register-a-phone-number`, accessed 2020-09-01.

[339] 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, 2018.

[340] Rachee Singh, Rishab Nithyanand, Sadia Afroz, Paul Pearce, Michael Carl Tschantz, Phillipa Gill, and Vern Paxson. Characterizing the nature and dynamics of tor exit blocking. In *26th USENIX Security Symposium*, pages 325–341, 2017.

[341] Scott Skinner-Thompson. *Privacy at the margins*. Cambridge University Press, 2021.

[342] Paul Slovic. Perception of risk. *Science*, 236(4799):280–285, 1987.

[343] Robert Snell. Feds use anti-terror tool to hunt the undocumented. The Detroit News, May 2017. https://www.detroitnews.com/story/news/local/detroit-city/2017/05/18/cell-snooping-fbi-immigrant/101859616/, accessed 2021-01-10.

[344] Daniel J. Solove. A Taxonomy of Privacy. *University of Pennsylvania Law Review*, 154(3):477, January 2006.

[345] Nivedita Sriram. Dating data: Lgbt dating apps, data privacy, and data security. *University of Illinois Journal of Law, Technology & Policy*, 2020(2):507–528, 2020.

[346] Angelika Strohmayer, Jenn Clamen, and Mary Laing. Technologies for social justice: Lessons from sex workers on the front lines. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 2019.

[347] Angelika Strohmayer, Mary Laing, and Rob Comber. Technologies and social justice outcomes in sex work charities: Fighting stigma, saving lives. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, 2017.

[348] Carola Suárez-Orozco, Marcelo M. Suárez-Orozco, and Irina Todorova. *Learning a New Land: Immigrant Students in American Society*. Harvard University Press, 2009.

[349] Kaiwen Sun, Carlo Sugatan, Tanisha Afnan, Hayley Simon, Susan A. Gelman, Jenny Radesky, and Florian Schaub. “they see you’re a girl if you pick a pink robot with a skirt”: A qualitative study of how children conceptualize data processing and digital privacy risks. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, CHI ’21, New York, NY, USA, 2021. Association for Computing Machinery.

[350] Latanya Sweeney. Discrimination in online ad delivery: Google ads, black names and white names, racial discrimination, and click advertising. *Queue*, 11(3):10–29, mar 2013.

[351] TAMPEP. Sex Work Migration Health. A report on the intersections of legislations and policies regarding sex work, migration and health in Europe. Technical report, TAMPEP International Foundation, 2009.

[352] Linnet Taylor, Luciano Floridi, and Bart van der Sloot, editors. *Group Privacy*. Springer International Publishing, 2017.

[353] Paul Taylor, Mark H. Lopez, Jeffrey S. Passel, and Seth Motel. Unauthorized immigrants: Length of residency, patterns of parenthood. Pew Hispanic Center, 2011.

[354] Telegram. Telegram faq - phone number, no date. https://telegram.org/faq#q-i-have-a-new-phone-number-what-do-i-do, accessed 2020-09-01.

[355] The American Civil Liberties Union of Vermont. Aclu demands immediate end to dmv facial recognition program. Press Release, May 2017. [Online; Retrieved 17 September 2017].

[356] The Spamhaus Project. `https://www.spamhaus.org/statistics/countries`.

[357] The White House. Executive order 13767, January 2017. [Online; Retrieved 17 September 2017].

[358] The White House. Executive order 13768, January 2017. [Online; Retrieved 17 September 2017].

[359] The White House. Executive order 13769, January 2017. [Online; Retrieved 17 September 2017].

[360] K. Thomas, D. Akhawe, M. Bailey, D. Boneh, E. Bursztein, S. Consolvo, N. Dell, Z. Durumeric, P. Kelley, D. Kumar, D. McCoy, S. Meiklejohn, T. Ristenpart, and G. Stringhini. Sok: Hate, harassment, and the changing landscape of online abuse. In *2021 IEEE Symposium on Security and Privacy (SP)*, 2021.

[361] Sadegh Torabi and Konstantin Beznosov. Sharing health information on facebook: Practices, preferences, and risk perceptions of north american users. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, pages 301–320, Denver, CO, June 2016. USENIX Association.

[362] Kentaro Toyama. *Geek Heresy: Rescuing Social Change from the Cult of Technology*. PublicAffairs, 2015.

[363] Marketa Trimble. *Geoblocking, Technical Standards and the Law*, chapter 947. Scholarly Works, 2016. `http://scholars.law.unlv.edu/facpub/947`.

[364] Jenny Hsin-Chun Tsai. Use of computer technology to enhance immigrant families' adaptation. *Journal of Nursing Scholarship*, 38(1):87–93, 2006.

[365] Michael Carl Tschantz, Sadia Afroz, Shaarif Sajid, Shoaib Asif Qazi, Mobin Javed, and Vern Paxson. A bestiary of blocking: The motivations and modes behind website unavailability. In *8th USENIX Workshop on Free and Open Communications on the Internet (FOCI 18)*, Baltimore, MD, 2018. USENIX Association.

[366] Joseph Turow, Michael Hennessy, and Nora Draper. *The Tradeoff Fallacy: How Marketers are Misrepresenting American Consumers and Opening Them up to Exploitation. Report*. Annenberg School of Communication, University of Pennsylvania, 2015.

[367] Twitter. About your email and phone number discoverability privacy settings, no date. `https://help.twitter.com/en/safety-and-security/email-and-phone-discoverability-settings`, accessed 2020-09-01.

[368] Twitter. Personal information and ads on twitter, no date. https://help.twitter.com/en/information-and-ads, accessed 2020-08-22.

[369] Blase Ur, Patrick Gage Kelley, Saranga Komanduri, Joel Lee, Michael Maass, Michelle L. Mazurek, Timothy Passaro, Richard Shay, Timothy Vidas, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. How does your password measure up? the effect of strength meters on password creation. In *Proceedings of the 21st USENIX Conference on Security Symposium*, Security'12, pages 5–5, Berkeley, CA, USA, 2012. USENIX Association.

[370] G. Venkatadri, A. Andreou, Y. Liu, A. Mislove, K. P. Gummadi, P. Loiseau, and O. Goga. Privacy risks with facebook's pii-based targeting: Auditing a data broker's advertising interface. In *2018 IEEE Symposium on Security and Privacy (SP)*, pages 89–107, USA, May 2018. IEE.

[371] Sarah Vieweg and Adam Hodges. Surveillance & modesty on social media: How qataris navigate modernity and maintain tradition. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing*, CSCW '16, page 527–538, New York, NY, USA, 2016. Association for Computing Machinery.

[372] Edna A. Viruell-Fuentes. Beyond acculturation: Immigration, discrimination, and health research among mexicans in the united states. *Social Science & Medicine*, 65(7):1524–1535, Oct 2007.

[373] Jessica Vitak. The impact of context collapse and privacy on social network site disclosures. *Journal of Broadcasting & Electronic Media*, 56(4):451–470, 2012.

[374] Jessica Vitak and Jinyoung Kim. "you can't block people offline": Examining how facebook's affordances shape the disclosure process. In *Proceedings of the 17th ACM Conference on Computer Supported Cooperative Work & Social Computing*, CSCW '14, pages 461–474, New York, NY, USA, 2014. ACM.

[375] Jessica Vitak, Yuting Liao, Mega Subramaniam, and Priya Kumar. 'i knew it was too good to be true": The challenges economically disadvantaged internet users face in assessing trustworthiness, avoiding scams, and developing self-efficacy online. *Proc. ACM Hum.-Comput. Interact.*, 2(CSCW), nov 2018.

[376] Kaveh Waddell. 'give us your passwords'. *The Atlantic*, February 2017. [Online; Retrieved 17 September 2017].

[377] Kurt Wagner and Jason Del Ray. Facebook's 'people you may know' feature can be really creepy. how does it work? Vox, October 2016. https://www.vox.com/2016/10/1/13079770/how-facebook-people-you-may-know-algorithm-works, accessed 2020-10-07.

[378] Zack Wallace. How to block entire countries from accessing your website. SitePoint, April 2015. https://www.sitepoint.com/how-to-block-entire-countries-from-accessing-website/.

[379] Yang Wang, Pedro Giovanni Leon, Alessandro Acquisti, Lorrie Faith Cranor, Alain Forget, and Norman Sadeh. A field trial of privacy nudges for facebook. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '14, pages 2367–2376, New York, NY, USA, 2014. ACM.

[380] Yang Wang, Gregory Norcie, Saranga Komanduri, Alessandro Acquisti, Pedro Giovanni Leon, and Lorrie Faith Cranor. "i regretted the minute i pressed share": A qualitative study of regrets on facebook. In *Proceedings of the Seventh Symposium on Usable Privacy and Security*, SOUPS '11, pages 10:1–10:16, New York, NY, USA, 2011. ACM.

[381] N. Warford, T. Matthews, K. Yang, O. Akgul, S. Consolvo, P. Kelley, N. Malkin, M. L. Mazurek, M. Sleeper, and K. Thomas. Sok: A framework for unifying at-risk user research. In *2022 2022 IEEE Symposium on Security and Privacy (SP) (SP)*, pages 1545–1545, Los Alamitos, CA, USA, may 2022. IEEE Computer Society.

[382] Mark Warner, Andreas Gutmann, M. Angela Sasse, and Ann Blandford. Privacy unraveling around explicit hiv status disclosure fields in the online geosocial hookup app grindr. *Proc. ACM Hum.-Comput. Interact.*, 2(CSCW), nov 2018.

[383] Tom Warren. ios 11 has a 'cop button' to temporarily disable touch id. The Verge, Aug. 17, 2017, 2017. accessed: Sept. 17, 2017.

[384] Miranda Wei, Maximilian Golla, and Blase Ur. The password doesn't fall far:how service influences password choice. *Proceedings of the Who Are You?! Adventures in Authentication 2018 Workshop (WAY)*, 4th WAY, 2018.

[385] WhatsApp. How to verify your number, no date. `https://faq.whatsapp.com/iphone/verification/how-to-verify-your-number`, accessed 2020-09-01.

[386] Alma Whitten and J. D. Tygar. Why johnny can't encrypt: A usability evaluation of pgp 5.0. In *Proceedings of the 8th Conference on USENIX Security Symposium*. USENIX Association, 1999.

[387] Philipp Winter, Anne Edmundson, Laura M. Roberts, Agnieszka Dutkowska-Zuk, Marshini Chetty, and Nick Feamster. How do tor users interact with onion services? *Proceedings of the 27th USENIX Security Symposium*, 2018.

[388] Pamela Wisniewski, Heather Lipford, and David Wilson. Fighting for my space: Coping mechanisms for sns boundary regulation. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2012.

[389] Jill Palzkill Woelfer and David G Hendry. Homeless young people's experiences with information systems: life and work in a community technology center. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 1291–1300. ACM, 2010.

[390] Maria Xynou, Arturo Filastò, and Simone Basso. Measuring internet censorship in cuba's parknets. `https://ooni.torproject.org/post/cuba-internet-censorship-2017/`, 2017.

[391] Svetlana Yarosh. Shifting dynamics or breaking sacred traditions? the role of technology in twelve-step fellowships. In *Proc. Conference on Human Factors in Computing (CHI '13)*. ACM, 2013.

[392] Hirokazu Yoshikawa. *Immigrants Raising Citizens: Undocumented Parents and Their Children*. Russell Sage Foundation, 2011.

[393] Reza Zafarani, Mohammad Ali Abbasi, and Huan Liu. *Social media mining: an introduction*. Cambridge University Press, 2014.

[394] Jun Zhao, Ge Wang, Carys Dally, Petr Slovak, Julian Edbrooke-Childs, Max Van Kleek, and Nigel Shadbolt. 'i make up a silly name': Understanding children's perception of privacy risks online. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, CHI '19, page 1–13, New York, NY, USA, 2019. Association for Computing Machinery.

[395] Yan Zhao, Shiming Li, and Liehui Jiang. Secure and efficient user authentication scheme based on password and smart card for multiserver environment. *Security and Communication Networks*, 2018:1–13, 05 2018.

[396] Philip R. Zimmermann. *The Official PGP User's Guide*. MIT Press, Cambridge, MA, USA, 1995.

[397] Jonathan Zittrain and Benjamin Edelman. Internet filtering in China. *IEEE Internet Computing*, 7(2):70–77, 2003.

[398] Yixin Zou, Abraham H. Mhaidli, Austin McCall, and Florian Schaub. "i've got nothing to lose": Consumers' risk perceptions and protective actions after the equifax data breach. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, pages 197–216, Baltimore, MD, August 2018. USENIX Association.

[399] Shoshana Zuboff. *The age of surveillance capitalism: the fight for a human future at the new frontier of power*. PublicAffairs, first edition edition, 2019.