Aunties, Strangers, and the FBI: Online Privacy Concerns and Experiences of Muslim-American Women

Tanisha Afnan and Yixin Zou, *University of Michigan School of Information;* Maryam Mustafa, *Lahore University of Management Sciences;* Mustafa Naseem and Florian Schaub, *University of Michigan School of Information*

https://www.usenix.org/conference/soups2022/presentation/afnan

This paper is included in the Proceedings of the Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022).

August 8–9, 2022 • Boston, MA, USA

978-1-939133-30-4

Open access to the Proceedings of the Eighteenth Symposium on Usable Privacy and Security is sponsored by USENIX.

Aunties, Strangers, and the FBI: Online Privacy Concerns and Experiences of Muslim-American Women

Tanisha Afnan[1] Yixin Zou[1] Maryam Mustafa[2] Mustafa Naseem[1] Florian Schaub[1]
[1]*University of Michigan School of Information* [2]*Lahore University of Management Sciences*

Abstract

Women who identify with Islam in the United States come from many different race, class, and cultural communities. They are also more likely to be first or second-generation immigrants. This combination of different marginal identities (religious affiliation, gender, immigration status, and race) exposes Muslim-American women to unique online privacy risks and consequences. We conducted 21 semi-structured interviews to understand how Muslim-American women perceive digital privacy risks related to three contexts: government surveillance, Islamophobia, and social surveillance. We find that privacy concerns held by Muslim-American women unfolded with respect to three dimensions of identity: as a result of their identity as Muslim-Americans broadly (e.g., Islamophobic online harassment), as Muslim-American women more specifically (e.g., reputational harms within one's cultural community for posting taboo content), and as a product of their own individual practices of Islam (e.g., constructing female-only spaces to share photos of oneself without a hijab). We discuss how these intersectional privacy concerns add to and expand on existing pro-privacy design principles, and lessons learned from our participants' privacy-protective strategies for improving the digital experiences of this community.

1 Introduction

Islam is the fastest growing religion in the United States [32]. Despite Islam's growing role and presence in U.S. history, Muslim communities in the U.S. have to contend with discrimination, prejudice, and mass surveillance [20, 47, 50, 68]. Muslim-American women are further subjected to a unique set of targeted attacks and stereotypes while also facing heightened vulnerability related to gender-specific veiling practices (such as the hijab), which act as visible identifiers of Islam [30, 99]. Western narratives paint Muslim women as meek, oppressed, and complicit in their own apparent subjugation [48, 64, 76]. These attributes can result in serious consequences in various contexts, such as hiring discrimination [4, 16]. Additionally, within their own religious and cultural communities, Muslim women might face restrictive gender norms and behavioral expectations, leaving them vulnerable to social consequences if transgressed. These stereotypes, coupled with implications related to other marginalized identities such as immigration status, race, and gender, mean that Muslim-American women may need more specific ways to control their information and own their narratives.

While privacy has been studied extensively [15, 27, 55, 71], the particular concerns and circumstances of Muslim women are relatively understudied. Prior work at the intersection of Muslim experiences and human-computer interaction (i.e., Islamic HCI), while offering rich insights into some of this community's experiences [1, 2, 80, 81, 100], often centers on Muslim women residing in Muslim-majority countries. Our research expands on existing Islamic HCI literature by exploring the additional challenges and perspectives of Muslim women living in countries where Muslims are a minority group, specifically in the United States. Prior research also reveals how an individual's level of religious adherence may influence their preferences and behaviors [58, 66, 67, 107]. We are interested in understanding to what extent individual religiosity (particularly how tenets of Islam, which often prescribe heightened values of modesty to women [2, 34]) may shape how Muslim-American women navigate their online privacy concerns.

To understand if and how Muslim-American women experience privacy concerns, we interviewed 21 Muslim-American women about their typical tech consumption, privacy-protective behaviors and strategies, and scenario-specific privacy concerns. Our findings show that privacy concerns held by Muslim-American women manifest in three distinct

USENIX Symposium on Usable Privacy and Security (SOUPS) 2022.
August 7–9, 2022, Boston, MA, United States.

dimensions. First, participants expressed privacy concerns as a result of identifying as Muslim-American broadly. Participants described deliberately choosing when and where to disclose this identity and how such disclosure could pose risks to them (e.g., feeling the need to constantly moderate their speech even in personal text messages, because a government agent may be monitoring them). Second, participants identified concerns about potential harms as a result of identifying more specifically as Muslim-American *women* (e.g., being held to higher scrutiny by their cultural community for sharing photos of themselves hanging out with individuals of the opposite gender). At the third and most personal level, participants' individual religiosity and relationship to Islam also shaped their privacy concerns and behaviors. Participants who described themselves as more deeply religious were more likely to have more private online presences (e.g., sharing fewer photos of themselves), but all of our participants' privacy preferences were shaped by their lived experiences as Muslim-Americans broadly and Muslim-American women specifically.

Our participants also shared key strategies they have adopted to mitigate their concerns (e.g., creating female-only spaces on social media to share more intimate content) and noted how existing technology does not meet their privacy needs. We discuss implications of our findings, including an intersectional lens in conceptualizing privacy and design recommendations for better addressing the privacy needs of Muslim-American women.

Researcher Positionality. Our research team consists of members with both insider and outsider perspectives, which contributed to our analysis approach and understanding of findings. Three authors identify as Muslim. Three authors identify as women, and two of them as Muslim women. The authors have diverse cultural backgrounds and religious attitudes, including Muslim women who wear the hijab and those who do not. The first author, who conducted all interviews, identifies as a cisgender Muslim-American woman.

2 Related Work

We examine existing research on Muslims in America, women and privacy in Islam, and the privacy risks Muslim women face.

2.1 Muslims in America

Muslims have been historically othered in America as a religious minority. Islamophobia, the specific prejudice against and hatred towards Muslims, surged after the 9/11 terrorist attacks [33, 50, 76, 94]. Since then, Muslims have often been portrayed by the media with "continuous reference to images of extremism, terrorism, and irrationality" [94]. Respective portrayals delineate the American 'us' and the alien 'them,' perpetuating a conflict for Muslim Americans who must reconcile these two seemingly disparate parts of their identity. Hijab, a veil or headscarf worn publicly by some Muslim women, is a highly visible identifier of Islam. This makes hijab-wearing Muslim women particularly vulnerable targets of hate speech and crimes [76] while exposing them to gendered perceptions such as the stereotype of "oppressed Muslim woman" [87]. Through a Western lens, the image of a veiled female represents the subordination of women, falsely rendering Muslim women as either content in their disenfranchisement or in need of rescue [30].

The hypervisibility of Muslims in the U.S., due to amplified media depictions following 9/11, gave rise to growing "Muslim self-consciousness" [47, 91] and efforts to 'repackage' and 'rebrand' the Muslim identity to be more appetizing to Western values and norms. Muslim Americans may purposefully choose which aspects of themselves are publicly visible to distance themselves from the 'Muslim' label, e.g., by framing abstention from alcohol in social settings as a health-related concern rather than a religious conflict [91]. A more overt approach, often employed by community leaders, is to construct a 'modern and moderate' Muslim-American identity to be more compatible with American norms [78]. This approach ranges from smaller, self-policing behaviors (e.g., wearing 'friendlier' pink hijabs rather than more stigmatized black hijabs) to larger decisions such as moving to predominantly white neighborhoods [20, 91]. In our study, we explore how the Muslim-American identity conflict manifests in digital spaces, and how the mainstream stigmatization of Islam affects participants' privacy concerns and experiences online.

2.2 Women and Privacy in Islam

Religiousness, or the degree to which an individual adheres to the tenets of their religion, may also influence one's privacy needs, concerns, and behaviors. Prior research has studied religiousness in healthcare and consumer behavior [58,66,67,107]. Higher levels of religious involvement have been shown to have positive correlation with psychological well-being [67], but can also be deterrents for seeking treatment for stigmatized diseases such as HIV [74]. Religious individuals are less likely to be impulsive shoppers [58], more likely to orient along traditional gender lines in purchases [107], and more likely to exhibit brand or quality consciousness [66]. In studies measuring religious involvement, women (compared to men) and individuals of racial/ethnic minority groups consistently have higher scores [57].

In our study, we explore how Islamic conceptualizations of privacy might influence privacy concerns and behaviors of Muslim-American women. Western conceptualizations of privacy tend to center individual freedoms [105]. By contrast, privacy in Islam is tied to ideals of modesty and family honor, often extending beyond the personal self [34]. Muslim women carry additional responsibilities to uphold their family's reputation via their own individual actions and opinions. The concept of preserving family honor is

unevenly laid on Muslim women more than men [77, 80, 100], as reflected by Muslim women's stricter privacy practices on social media platforms [1, 2]. Three notions of privacy are described in the Qu'ran [2]: the *awrah* represents the most intimate or private spaces that must be shielded from others (e.g., parts of a woman's body), the *hurma* represents pure and sacred 'spaces' that must be protected to preserve their sanctity (e.g., the family home), and the *haq al-khososyah* is one's right and responsibility to protect both their awrah and hurma through actions. Although Muslim women in the U.S. have roots in many different ethnic and cultural communities, acknowledging the interplay between gender, modesty and privacy in Islam is important for best understanding the values and attitudes of Muslim-American women. Privacy concerns as a result of gendered Islamophobia [30,76] may further affect Muslim-American women's online disclosures and behaviors.

2.3 Muslim Women's Privacy Risks

For Muslim women, the main types of perceived threats discussed in media and prior work include social consequences within the Muslim community, government surveillance, and Islamophobia. As such, we base our interview protocol on these scenarios.

2.3.1 Social risk factors within community

Muslim women's behaviors are often linked to their honor, and by extension, the honor of their families. When behaviors outside of cultural norms are discovered, erring individuals are subject to reputational harms within their communities. *Haram* behaviors, or behaviors not considered permissible by Islam, vary by community but typically include alcohol consumption, engaging in romantic relationships outside of marriage, privately communicating with individuals of the opposite gender, and getting tattoos [8]. Social media pose further privacy risks, requiring Muslim women to consider what information to make public and how their online content may be interpreted. In a study with Muslim-Kuwaiti youth, participants described "shame and loss of face" due to information exposure on social media and exhibited conservative usage as a result [34]. In another study with Muslim-Qatari women, participants viewed Facebook as a medium for simple correspondences rather than a space for deeper self-expression, and actively considered social repercussions of sharing content online that could be misunderstood as haram behavior [53].

For Muslim women living in Western societies such as Muslim-American women, online behaviors become further complicated as they must reconcile conflicting cultural values of 'mainstream' society with certain conventions of Islam. For example, Abokhodair and Vieweg document a scenario in which a Muslim woman grappled with the decision of accepting a male coworker's Facebook friend request to be sociable or rejecting it out of obligation to family expectations [2]. Social media has become a challenging terrain to navigate for Muslim women who want to engage in different behaviors that correlate with different facets of their lives. This struggle aligns with prior research on context collapse, i.e., multiple social circles with varying norms become flattened into a singular audience on social media [56, 101]. Strategies for coping with context collapse are often burdensome, and individuals may opt to mute certain disclosures entirely [26, 31]. In our work, we sought to understand the role of context collapse and specific cultural or religious expectations on Muslim-American women's online behaviors. Though participants assigned varying levels of significance to these factors, they influenced and constrained all of our participants' digital activities.

2.3.2 Fear of government and military surveillance

Government actors are recognized as one of the largest threats to the Muslim-American community due to their history of targeted surveillance [20, 47, 50, 92]. Following 9/11, Muslim-Americans have been subjected to institutional surveillance on local and national levels. The PATRIOT Act, a counterrorism act drafted in response to 9/11, ushered in a new era of surveillance programs by law enforcement targeting Muslims. For instance, the New York City Police Department's Muslim Surveillance Program targeted Muslim-American communities in the city via undercover operations, secret informants, and other deceptive and invasive tactics [50]. The Pentagon's Total Information Awareness System (TIA) was another predictive counterterrorism system aggregating data on individuals who may pose future terrorist threats, namely immigrants, Muslims, and other communities of interest. TIA data came from various sources, including financial and medical records, educational records, familial associations, and commercial data such as online shopping histories [68]. This expansion of government capabilities infringed on the civil liberties and rights of many Muslim Americans [33] while deepening mistrust between the American public and its Muslim communities.

In response to rising government surveillance, Muslim American communities exhibited drastic chilling effects in their online and offline behaviors [42, 44, 92]. Though many programs have been dismantled since, new surveillance efforts, claiming to no longer targeting Muslim and Arab communities, continue to make government tracking a relevant concern [9]. Emerging technologies allow for new avenues of data collection [104]. The US military, for example, is known to purchase location data of users from various smartphone apps; some of the data has been used to launch and plan drone attacks in Muslim-majority countries [86]. More recently, such trading of user data raised criticism among Muslim Americans when it was revealed that Muslim Pro, a mobile app for Islamic prayer times, was believed to have sold user data to the U.S. Special Operations Command through data broker intermediaries [17]. We explored the scenario of U.S. government and military surveillance in our study and found several tactics employed

by our participants to address related concerns.

2.3.3 Islamophobia online

Blatant Islamophobia, i.e., explicit hate crimes and speech targeted at Muslims, is prevalent online [12, 13]. Movement towards white nationalism following the 2016 U.S. elections has contributed to an increase in xenophobic behaviors towards Arabs and other Muslim-Americans [106]. Muslim women, particularly those wearing hijab, remain visible targets of these attacks online [48, 64, 76], leaving many vulnerable to assaults on their physical and psychological safety.

Latent Islamophobia, i.e., prejudice against Muslims enacted in implicit ways, can also thrive online [46]. Research on how social media data particularly affects job seeking Muslim-Americans suggests that screening practices have a discriminatory impact on their employability [16]. A hiring discrimination experiment in the U.S. found that Muslim job applicants, who were only identifiable as Muslim on their social media profiles, "received 38 percent fewer e-mails and 54 percent fewer phone calls" than replicated candidates with other religious affiliations [102]. Another study similarly revealed that applicants who had disclosed their Muslim-American identity on social media received 16% fewer callbacks than the identical Christian candidate in specific regions. This influence of online disclosure on U.S. firms' hiring practices is an important reality to consider in studying Muslim-American women's online behaviors.

3 Research Method

Prior work has primarily focused on Muslim women living in Muslim majority contexts [1, 2, 34, 97, 100]. In our study, we focused on the experience of Muslim women in the U.S., who additionally have to contend with being targets of mass surveillance, Islamophobia, and media stigmatization, among other concerns [33, 50, 76, 77, 92]. We explored how these factors affect Muslim-American women's online privacy concerns and experiences.

3.1 Study Design

As Muslim-American women are a relatively understudied population, we opted for a qualitative approach. The first author conducted 21 semi-structured interviews between May and August 2021. Our study was approved by the University of Michigan's Institutional Review Board (IRB).

Interested individuals were directed to complete a pre-study survey (see Appendix A), asking for demographic information, which we used to contextualize our sample. After completing the pre-survey, participants were invited to share their availability and given a written consent form to complete prior to their interview session. All interviews were conducted remotely via Zoom in English.

Each interview (see Appendix B for the interview script) began with questions to build rapport and gauge the participant's daily tech use, followed by general questions about tech-related concerns, privacy and their faith. In the second part, we asked scenario-specific questions about four major categories of privacy risks—ad tracking, social surveillance, U.S. government surveillance, and Islamophobia. Our questions were informed by related work examining experiences of Muslim women (primarily in Muslim-majority countries), Muslim-Americans broadly, and women of color in the U.S. (see Section 2). Our goal was to bring these often separate conversations together. Participants were given the opportunity to discuss their personal concerns in Part 1 before being asked about these scenarios in Part 2; almost all participants mentioned at least one of the scenarios unprompted. At the end, we gave participants opportunity to share concerns not yet captured.

After the interview, participants completed an exit survey (see Appendix C) that consisted of the 5-item Islam-specific version of the Centrality of Religiosity scale [43] to measure their level of religious adherence, complementing what was shared during the interview. We slightly rephrased one question for better fit and added another, taking inspiration from the Pew Research Center's work [65]. Upon completion of the exit survey, participants received a $20 virtual gift card. Interviews lasted 67 minutes on average, ranging from 41 to 95 minutes.

3.2 Recruitment and Demographics

We sought adult participants who identified with the religion or culture of Islam, had a permanent home in the U.S., and were regular technology users. We also asked about immigration status but did not screen participants based on it. We advertised our study through social media in relevant online groups (e.g., Muslim Women's Professional Network), by partnering with Islamic organizations (e.g., the Sister's Committee at a local mosque), and snowball sampling. Leaders at the community organizations we collaborated with also served as pilot interviewees and provided valuable feedback on our interview protocol. While we did not record the exact channel each participant was recruited from, we did not observe concentration in any particular channel. Only two participants were recruited via snowball sampling. The first author kept recruiting participants and conducting interviews until reaching saturation [24].

Table 1 provides an overview of participant demographics. Our study captured the experiences of a specific subset (young and highly-educated professionals) of Muslim-American women. While this focus limits the generalizability of our findings, our study contributes new insights into the unique privacy experiences of this population. Participants were 22 to 39 years old (mean 28 years). All were college graduates, and 11 held graduate degrees. Participants exhibited similar levels of daily screen-time and tech use. Annual household income varied from less than $25,000 to over $150,000. Thirteen participants identified as South/Southeast Asian (Pakistani,

Table 1: Participant demographics

ID	Age	CRS	Education	Ethnicity
P01	39	3.8	Master's Degree	South Asian
P02	27	4.8	Master's Degree	MENA
P03	26	3.6	Master's Degree	South Asian
P04	22	2.8	Bachelor's Degree	South Asian
P05	34	4.8	Professional Degree	South Asian
P06	29	4.4	Master's Degree	South Asian
P07	25	4.4	Bachelor's Degree	MENA
P08	25	4.2	Master's Degree	South Asian
P09	25	4.8	Master's Degree	MENA
P10	35	3.8	Master's Degree	MENA
P11	26	4.6	Bachelor's Degree	Black or African
P12	29	4	Master's Degree	Central Asian
P13	29	4	Master's Degree	South Asian
P14	37	4.6	Master's Degree	South Asian
P15	25	4.8	Master's Degree	South Asian
P16	24	3.8	Bachelor's Degree	South Asian
P17	30	4	Bachelor's Degree	South Asian
P18	N/A	2.4	Doctorate Degree	South Asian
P19	23	4.8	Professional Degree	South Asian
P20	27	5	Master's Degree	Central Asian
P21	28	4.2	Bachelor's Degree	Black or African

MENA = Middle East and North Africa.

Indian, Bangladeshi, Indonesian), four as Middle Eastern or North African, two as Central Asian (Afghanistan), and two as Black or African. Participants' CRS scores ranged from 2.4 to 5 (scale range is 1 to 5), skewing toward the higher end. Scores were calculated using responses from items 1-5 on the exit survey. The mean score of 4.17 maps to 'highly religious' [43]. We discuss the validity of these scores later in our findings.

3.3 Data Analysis

Interview sessions were audio recorded with Zoom. One participant asked not to be recorded, and the interviewer took notes instead. Recordings were transcribed using a transcription service. The research team reviewed transcripts to ensure consistency with the recordings. Throughout the data collection process, the research team met regularly to discuss the collected data.

We used an inductive approach [84] to analyze our interview data so that findings would not be constrained by our research questions. We used thematic analysis [19] to organize and interpret interview transcripts and notes. The first author began with theoretical memoing and affinity diagramming to familiarize themselves with the data, while noting initial reactions and ideas. The first author then conducted open, inductive coding across the entire dataset to develop a codebook. The research team then reviewed themes and preliminary codes to check for their relevance to the entire dataset. Themes were refined through further iterative rounds of coding. Final analysis focused on extracting illustrative examples for a cohesive narrative around our original research questions. Though the research team worked together to develop and evaluate codes throughout the analysis process, the first author coded the entire dataset themselves, therefore not requiring the calculation of inter-rater reliability [61].

3.4 Limitations

We chose an interview approach to gain insights into the privacy experiences of a relatively understudied group. This method also imposed certain constraints. Though our sample had diversity along some parameters such as income, we cannot claim that our sample is representative of the highly diverse population of Muslim-American women. Our sample primarily consists of young, highly educated Muslim-American women. The experiences highlighted in our study are only reflective of the lived experiences of those participants. This also differentiates our sample from Muslim woman populations studied in some prior research (i.e., women in the Global south with limited literacy [7, 10, 34, 80, 81]) and provides important insights about this subpopulation. Furthermore, the interviewer's identity as a Muslim-American woman may have made some participants more likely to disclose some details, but could also have introduced social desirability bias for others [54].

4 Findings

Our findings are organized based on three distinct dimensions of privacy concerns and the respective risks and harms experienced by our participants. First, participants shared privacy concerns tied to their identities as Muslims in the U.S., such as those related to targeted government surveillance. Second, participants described concerns associated with their identities more specifically as Muslim-American *women*, such as those related to gendered cultural norms. Lastly, individual religiosity and how participants practiced Islam (e.g., wearing a hijab) also shaped their online privacy concerns.

4.1 Privacy Concerns as Muslim-Americans

While participants held multiple intersecting minority identities, many related perceived privacy risks to their identity as Muslim-Americans. Participants viewed these risks as relevant to any Muslim-American regardless of gender, age, or other characteristics. Concerns centered on the U.S. government and military, strangers online, and companies.

4.1.1 Surveillance by the U.S. government and military

The most prominent concern, mentioned by almost all participants, was targeted surveillance by the U.S. government or military. While counterterrorism efforts targeting Muslims

emerged in the years immediately following 9/11 and many have been disbanded since, several participants described suspicion about the extent to which they were being monitored by the government. Participants recounted stories of invasive government practices they heard about from secondary sources (e.g., media outlets, podcasts) or from their own personal communities (e.g., a local mosque). Some participants described witnessing or experiencing negative actions by governmental entities (e.g., being disproportionately subjected to random TSA checks). P19 discussed how a suspected FBI agent had been monitoring and harassing community members at her mosque:

> "Basically the FBI sent a fake convert...to [my] masjid ...This guy would go to people's houses, befriend them, record their private conversations. He had a camera on one of the buttons of his shirt ...This guy would just bring up jihad [holy war in Islam] randomly and all the guys were like, 'Okay...' Eventually the masjid leadership ended up reporting this guy to the FBI and the FBI didn't do anything about it because they were like, 'Oh, it's our guy.' So the masjid got really suspicious." (P19)

Governmental counterterrorism efforts have been intentionally hidden [93]. With little verifiable information, many participants speculated that the government simply had access to 'everything,' i.e., any data about them in existence. Participants thought that the government's reach extended from public social media posts to private text messages. This concern of wide-reaching government access based on feelings of uncertainty has also been observed in other communities such as undocumented immigrants in the U.S. [39].

Additionally, participants often conflated what was accessible to private companies with what was accessible to the U.S. government or military. More than half of the participants expressed concerns about how their personal data may be exploited by private companies (e.g., companies profiting from targeted ads based on their personal data) as a generic privacy risk. Several participants further shared concerns about how private companies may share their information with the government. For instance, P10 highlighted the reported data flow from the Muslim Pro app to the U.S. military through data brokers:

> "This is scary for me...Because I belong to a certain group like being a Muslim person, I have to be watched. This is kind of a burden...especially [when] anything that you can type or write on social media can be used against you...Maybe I'm overreacting, but since the Muslim Pro app thing, when we all knew that they were selling our data to the biggest bidder, I've questioned a lot what I'm doing." (P10)

As a result of perceived targeted surveillance and concerns about how their data might be misused, many participants described experiencing chilling effects similar to those expressed by the Muslim community immediately after 9/11 [92]. This concern was exacerbated by the little autonomy participants felt they had against the entities in question. Most participants felt they had 'some' or 'little control' over information collected about them by private companies; 12 participants reported feeling 'no control' regarding information collected by the government.

Consequently, participants shared how they applied extra caution in day-to-day online and offline behaviors, such as avoiding posting about certain topics (e.g., political opinions critical of the U.S. government on Twitter). These chilling effects inhibited the degree to which participants felt they were able to freely express themselves online, meaningfully engage with others on social media, and consume media of interest. P14 shared why she adopted selective self-expression online:

> "I, as a Muslim, would not say certain words over text or even online just because I know that those are not good words to use...That would trigger [someone] to monitor and look into my profile and what I'm doing, and potentially have people tracking me. There are certain things that we do online that would elicit a greater response from other people. I think those types of things are flagged...It would be taken to a whole other level versus a white person looking that up..." (P14)

Fear of government surveillance has been documented as a common privacy concern across the U.S. adult population [98, 108, 109], and our findings indicate a continuing salient level of anxiety among Muslim-American women.

4.1.2 Islamophobia and strangers online

Online hate speech and harassment was another dominant risk participants linked to their identity as Muslim-Americans. Unlike concerns related to government or corporate entities, participants felt more equipped to protect themselves against threats from strangers online. To avoid hostile or unwanted attention, 19 participants described setting their social media accounts to private so that their content was only viewable by approved friends or followers. On platforms designed for public engagement, such as YouTube or TikTok, many participants opted to be passive spectators rather than active content creators, a behavior also mirrored in other exposure-sensitive populations [39, 59].

To avoid inciting hate speech from their approved friends and followers, participants curated audiences with whom they shared Islamic content (e.g., only sharing photos of them celebrating Eid with a subset of friends). Participants noted how their strategies evolved over time. P02 provides an example:

> "When I was a high schooler, I'd read maybe a Fox News post on Facebook, and then I would see people cussing out Muslims and I was so naive. I just thought I could convince them, so [I'd be] like, 'No, Muslims are good'...So in those parts of [social media], I experienced very Islamophobic

rhetoric. First it was like the replies back, and then I learned to just block [them], and then I learned after that to just not interact. Because there's no point essentially." (P02)

While such strategies offered participants relief from becoming targets of Islamophobia, many still regularly encountered Islamophobic sentiments shared online. Though not directed at them individually, this constant exposure to harassment still caused distress in their everyday Internet use.

4.2 Concerns as Muslim-American Women

In addition to the concerns linked to being Muslims in the U.S., participants shared concerns and risks specifically tied to being Muslim-American *women*. Many of these risks were described to be equally motivated culturally and religiously, with some participants describing them as results of "outdated patriarchal values" (P18). Participants spoke at length about deep gendered divides in expectations between men and women within their communities. Almost all participants noted that expectations and consequences Muslim men were subject to were significantly different from those for Muslim women. P07 unpacked these uneven cultural gender norms:

"I think Muslim women probably have to be a lot more careful. Because we're definitely judged more harshly. I think men can get away with a lot more, and not get judged for it. The actions they take, [they] don't see him as like, 'oh, this is going to ruin your life' in the way that conversations happen with females in our community. That's how it feels. Like you've ruined your life with this thing. So I think the ways that our communities interact with us is very different." (P07)

While participants expressed being adept in dealing with Islamophobic strangers, they reacted differently when asked about navigating online spaces they shared more closely with their cultural and religious communities. Social surveillance [34, 53] was a phenomenon that almost all participants immediately recognized and felt subjected to. Feeling pressured to accept the friend requests of those in their extended communities out of social obligation, while dealing with the consequences of context collapse [26, 31, 56], greatly limited how participants shared content even on their private social media profiles.

4.2.1 Social taboos and inappropriate content

Definitions of appropriate content to share online varied depending on participants' specific circumstances. For example, a participant who grew up in an area with a large Muslim population and attended an Islamic high school, shared concerns about critiquing a popular Islamic scholar on her personal social media. By contrast, a different participant, who grew up as the only Muslim-American in town, worried about untagging herself from photos in which she was holding a wine glass. The broad recurring categories of taboo content included photos with members of the opposite gender, photos that placed the participant in potentially inappropriate venues such as bars, photos of wearing clothes that could be considered immodest (e.g., ranging from wearing the hijab too loosely to wearing a bikini on the beach), content about romantic or intimate relationships, and sharing personal opinions on topics that participants felt Muslim women were not typically vocal about (e.g., mental illnesses).

While tensions between cultural and religious expectations of Muslim women and their online behaviors have been reported in prior work [1, 2, 80], our participants faced the added burden of navigating these cultural and religious expectations in a society with differing ideals. Trying to assimilate into western norms to subvert negative stereotypes [38, 94, 99] while upholding the cultural values of Islam left many participants distressed. For example, P01 described following behaviors similar to other American women while being cautious about her representation around family members:

" A lot of times you lead the double life. Not in a bad way, but I don't feel like I'm very different from most other American women because I pretty much do the same thing a lot of American women do. I dress the same as them, I eat the same kinds of foods. I'm single, so I date as well. But I have to hide certain parts of that when I'm around my family because it's inappropriate, and I always have to be aware of what's acceptable culturally, so I can never really share who I am." (P01)

Participants tied these amplified tensions to their intersecting identities as both Muslim and American women. Multiple participants shared feeling they led 'double lives' and being unable to find spaces in which they could share their full existences.

4.2.2 Protective strategies on social media

Participants noted that failing gendered expectations could have several negative consequences. Most concerning was the fear of reputational harm, which would affect participants personally as well as those around them. As P09 explained, "[It's an] obsession with their image. You're a Muslim woman. You can't do this. You're representing our whole community." Participants emphasized that the degree of potential harm depended on each individual family. Six participants had experienced *actual* social repercussions from sharing 'taboo content' on social media, while nine noted that they had not but were still deeply wary of the potential consequences. Participants mainly shared the fear of ostracism; other less commonly noted harms included explicit harassment and physical threats. Though risk does not always lead to tangible harms (e.g., in the form of financial loss), participants' perception of risks should not be dismissed as prior work has noted that perceived risk itself can

simultaneously create harm by affecting one's autonomy and psychological state (e.g., through chilling effects) [23].

To avoid these harms while still engaging in sincere self-expression, participants shared various strategies to create boundaries online. A common strategy was to use multiple social media profiles. All of our participants were active social media users and had accounts on at least three platforms. Having more than one platform meant that participants could add particularly judgemental community members on a selective set of social media accounts while hiding their profiles on others. Those most likely to pose threats typically included older extended family members and religious elders, who usually only used Facebook. As a result, some participants aligned their Facebook appearances more closely with the expectations of their communities while creating more authentic representations of themselves on other platforms like Twitter or Instagram. P12 provides an example:

> "Facebook definitely gets the more conservative, modest, professional aspects of me, because not only is that my friends, but it's also family. I have some family that are really strict...Not much goes to Facebook, and if things do go into Facebook, they're still very modest, very conservative, very clean post in aspects of what I wanted to post." (P12)

Some participants also took steps to limit the content others could see on the accounts they shared with those in their community. Examples included using options for restricted audiences (e.g., the close friends feature on Instagram), configuring privacy settings (e.g., locking their profiles on Facebook), and carefully vetting what kinds of content they posted. P06 described having a 'no-list' of friends on Facebook who had limited visibility of the content she posted:

> "I definitely had a list of people [on Facebook], I think it was just called my 'no-list' and it was just like family members that I felt like were a little...not trustworthy. I just felt like they would more like[ly] share things with older family members or other family members, and I just didn't really want to risk it... So if I posted a picture with me and all my friends at the beach, it was for everyone but my list of no people." (P06)

Despite best efforts, some participants shared experiences of data leakage, in which personal content they posted ended up reaching unintended viewers. P04 recounted how a photo in which she was tagged leaked to her family members and expressed her frustration with Facebook's privacy settings:

> "There's a time that I was wearing shorts in August in Austin, Texas...It was just me standing there with my friends. They took a photo. I was like, 'Oh, that's fine. They took the photo. What are they going to do, send it to my family?' But then they posted it on Facebook. I think it auto-tagged me...Somehow my settings were configured so that my friends can see the photos that I'm tagged in from other people. So, my family members had seen it because it was posted by someone else before I could notice and untag myself or delete it...I didn't know it was there until I logged in and I saw it was there. I would've preferred ... 'Hey, you're tagged in this photo. Do you want it to be on your timeline?' And it's up to me to say yes or no." (P04)

The desired feature P04 describes exists in Facebook but is not the default. Participants attributed many instances of unintended content sharing to the confusing choice architecture and privacy-unfriendly default settings on social media platforms, echoing existing privacy research on dark patterns around privacy controls [22, 41, 55]. Other participants attributed data leakage to individuals in their closer circles who might have exposed their content to others. Interface changes without sufficient notifications further pose barriers for participants to manage their content effectively, as P05 described:

> "I think Facebook changes how you have to adjust your privacy settings, like every six months. And you are like, 'what is this new thing I have to do? I have to click how many buttons and do X, Y or Z?"' (P05)

Ultimately, most participants felt they had more control over the personal information they shared with others on their private social media compared to limiting what data was available to companies and the government. However, control did not necessarily match concern levels. Though participants may have felt less control over the information collected about them by private companies, most participants expressed heightened anxiety over social consequences than surveillance capitalism by private companies [109]. This finding stands in contrast to the reported privacy concerns of 'general' American Internet users, who typically identify private companies as the biggest threat to their information [11].

4.3 Religiosity's Influence on Privacy Concerns

In addition to concerns tied to being Muslim-Americans and Muslim-American women, our findings suggest that differences in personal beliefs (e.g., what constitutes prayer), religious practices (e.g., veiling practices such as wearing a hijab), and involvement with Muslim-American communities and causes (e.g., the frequency of visiting a local mosque) all played a role in participants' conceptualization of privacy concerns and harms.

To better understand how religion influenced participants' privacy concerns and behaviors, we asked about each participant's religious practices during the interview; we also asked participants to complete an Islam-specific version of the CRS-5 [43]. The majority of our participants scored a 4 or higher on CRS-5 (mean 4.17), suggesting that our sample is 'highly religious.' However, the interview data revealed much greater variation and nuance in religiosity than what the CRS-5 results indicate. Individual participants' relationships with

religion were deeply personal and were not accurately captured by CRS-5. To understand this disconnect between qualitative and quantitative responses, consider participants P07 and P14. Both had similar CRS-5 scores (4.4 and 4.6) but described their religious practices quite differently. P07, while regarding herself as deeply spiritual, shared her deliberation of engaging in only a subset of practices that she felt comfortable with:

> "I think I'm a pretty deeply spiritual person and I've had a lot of back and forth in terms of how I like to practice with congregations...I've stepped away a lot from more organized practice...When I was in a bigger city where there was a lot more community, it just didn't always feel like the most comfortable. And when I was in very Muslim spaces, it didn't always feel like a great fit either, so I think I've moved away from things that are more established." (P07)

P14, on the other hand, shared her adherence to more traditional practices, and how visiting and engaging with her local mosque has always been important to her:

> "I do the simple [things] like greetings, [celebrating] the holidays, things like that...But I also grew up going to the mosque too, very regularly...And then, I moved around and I continued to always constantly go to the mosque, and even here now, where I live now, I do as well. That was a big part of my religion too, going to the mosque. That cultural aspect, that socialization, is a heavy part for me...Being part of a community, knowing that I'm part of a community too." (P14)

Based on this insight, we decided to focus our analysis on how participants described practicing Islam in the interviews and how they integrated religious practices into their daily lives. We found that more frequent intentional religious practices coincided with participants who defined privacy, in all regards, as an extremely important personal value. For example, participants who reported praying all five requisite prayers daily showed equal amounts of concern with regards to government surveillance, social surveillance, and surveillance capitalism. In contrast, participants who identified as Muslim more culturally (e.g., only praying on religious holidays) were more likely to show heightened concern for social surveillance, but exhibited signs of resignation or apathy [29] toward data collection practices of corporate entities, viewing them as a trade-off between privacy and convenience [11, 85]. For instance, P06 shared that she preferred having sufficient control over information shared on social media, but was willing to be tracked in other contexts such as shopping:

> "On social media, I like being able to exercise a certain modicum of control, just because different people can see different things...like different family members. I don't necessarily want everything out there all the time. I'd like opportunities to regulate that. And then in terms of other kinds of data, it would depend based on what it is. There's some data that I think is important for me to give...that makes things a whole lot easier, like for shopping...Tracking sometimes make[s] things easier and is more targeted. I just would like to exercise a little bit more control in that way, but to a certain degree. I think I'd be okay with giving up some autonomy too." (P06)

4.3.1 The impact of hijab

Veiling practices, as in whether or not a participant chooses to wear a head or face covering, substantially impacted participants' privacy concerns. All participants who wore hijab emphasized their autonomy and agency in wearing the hijab as a personal decision. Some wore the hijab as an act of visibility to present themselves as Muslim in all spaces, while others felt it aligned with their conceptions of Islamic privacy and their duty to protect their awrah [2]. Twelve participants mentioned potential consequences of wearing the hijab as a particular religious practice. Some of them felt that they were subjected to more scrutiny by other Muslims. As an example, P20 shared her frustration of having to contend with shaming around *how* one wears the hijab:

> "I think for a lot of Muslim women, there is a lot of constant conversation about hijab, what is hijab, how to wear hijab, how should you not wear it...blah, blah, blah. It's just ongoing. Often times I feel [it's a] very unhealthy conversation that really doesn't benefit anyone. And those conversations are driven by people who are not women...I think that's something a lot of Muslim women can relate to, having to deal with that from outside the community and within the community, being constantly critiqued." (P20)

Other participants noted that wearing the hijab might disadvantage them in interactions with non-Muslims. For example, hiring managers looking at an applicant's social media profiles would be able to conclude immediately that they were Muslim based on the hijab, and act in discriminatory ways [5, 48, 73].

While all participants who wore the hijab were proud of their choice and excited to represent themselves in digital spaces, they described how this decision also comes with costs. Our hijab-wearing participants shared unique strategies they adopted to navigate the nuances of appearing visibly Muslim online. Similar to some practices discussed earlier to keep judgemental community members at bay, participants leveraged multiple social media platforms. By dedicating different accounts for different purposes, participants were able to uphold certain outward images while still cultivating safe zones for more authentic expression. Snapchat was particularly popular for its ephemerality of posts, with a few participants sharing how they created women-only spaces with their closest friends on Snapchat to share photos of themselves without hijab.

In addition to managing multiple accounts with different content, our hijab-wearing participants shared other strategies to preserve their privacy when needed. Examples included

using images of inanimate objects or scenery as profile pictures, utilizing internal networks to crowdsource information for their needs (e.g., relying on Muslim Women's Professional Network instead of LinkedIn to look for jobs), and avoiding certain platforms that could be hostile spaces for Muslim women like themselves. P09 described her practice of selective disclosure and self-representation (showing the hijab or not) based on connections on the platform:

> "I already feel like I have a lot working against me being brown, being a hijabi...so I'm twice as cautious about what information I post or how I express my views, which is unfortunate because I am very outspoken and opinionated and still feel that fear. I have a Finsta with the girls and the gays that will see my hair. But I do not trust men. And so especially [on] Snapchat, where I have basically no men, I am more candid with what I will post there." (P09)

Although our participants varied in their veiling practices and respective motivations, participants shared consistently that wearing a hijab exposed them specific risks and vulnerabilities that were not experienced by Muslim women who chose not to physically veil and non-Muslim women.

4.3.2 Closeness to community and activism

Participants who engaged in public Muslim activism or relevant leadership expressed a particular subset of privacy considerations. These participants publicly advocated for specific social causes affecting Muslim communities online (e.g., on a public Twitter account) or offline (e.g. attending a protest), or have taken on public leadership roles in Islam-affiliated organizations (e.g., being the president of a Muslim students' association).

Supporting certain social causes, particularly those highlighting the plight of different Muslim communities, often placed participants on the side of issues that could be perceived as 'un-American' (e.g., critiquing the U.S. military in the war on terror). As a result, several participants shared how they had personally experienced privacy harms due to their activist work, ranging from targeted online harassment to more intense threats like doxing [96]. Such experience was particularly common when it came to controversial issues such as advocating for Palestinian liberation in discussions of the Israel-Palestine conflict. For instance, P02 shared her concern of being listed on Canary Mission, which keeps a blocklist of pro-Palestine activists, and how that might impact her job prospect:

> "Canary Mission is a website that [documents] anyone working in anything related to boycotting or divesting Israel, or is Pro-Palestine...They basically dox people on that website and employers look through that website, so then those people can't get jobs. That's something I am very careful [about] around my privacy or my identity anywhere. I do have separate accounts for different things...but if my face and name is on there, it opens you up to a lot of harassment." (P02)

Participants felt helpless with regards to these concerns and struggled to develop meaningful strategies to mitigate privacy risks associated with public Muslim activism other than opting for more low-effort and anonymous 'slacktivism' [82]. However, as P19 unpacked, hiding traces of engagement with Muslim activism is hard, and any slip-up could lead to severe reputational damage:

> "If you go to a protest, your name will be on there. You [might] just share a picture of you at a protest, right? Cool. You're supporting a really worthwhile cause. Meanwhile someone...could be like, 'Oh my God.' And then post you on their website and your job prospects gone, your social image tainted, people are calling you anti-Semitic, [or] they're calling you all these hurtful things that aren't true." (P19)

Ultimately, this left participants feeling as though they were at an impasse. Participants had to either curb their activist work or risk facing serious repercussions if they continued, a dilemma also echoed in the continued chilling effects of fears of government surveillance.

5 Discussion

Privacy needs are shaped by environmental, contextual, and individual factors [3, 55, 71, 75]. However, the privacy choices available in mainstream technology are often oriented along profit margins and the larger goals of private-interest companies. Privacy dark patterns are common among online service providers [18, 70], deceiving users into surrendering their personal information to maximize profit [109]. Value-sensitive design suggests that technological artifacts are not value-neutral and instead reflects the creators and communities they are borne from [36]. Even in cases where users' privacy needs are prioritized, technology developed and designed for a 'typical' user in the U.S. will deviate from the preferences of marginalized individuals and users across the globe [27, 108]. Prior Islamic HCI work, primarily situated in Muslim-majority countries, has recognized the role of Islam in users' interactions with digital technologies. Most notably, Islamic sociocultural norms, widely adhered to by Muslim families and individuals, can significantly impact how privacy is understood and put into practice (e.g., women consider their *awra* when posting photos of themselves) [2, 45, 69]. Our study shows how boundaries between Islamic norms and Western-influenced technology get blurred in the experiences of Muslim-American women — members of both mainstream American society and of their particular religious and cultural communities. Next, we discuss the crossroads of intersectionality and privacy, and outline design opportunities to support the needs of Muslim-American women.

5.1 Privacy Through an Intersectional Lens

Our findings align with similar concerns expressed by women in previous Islamic HCI research (e.g., upholding expectations of modest dressing by community elders [2, 45, 77]), but at heightened degrees because of our participants' intersecting identities as Muslim and American women. Our participants further contended with unique considerations due to their identity as Muslim women in the U.S. (e.g., being part of a stigmatized minority religion, being members of minority ethnic communities), and these tensions manifested in different ways involving a variety of actors. For some, the fear of government surveillance inhibited how they shared their political opinions on specific topics online. Some struggled with crafting an online presence that upheld the 'rules' enforced by their elders while reflecting their more 'American' sensibilities (e.g., debating whether to post a photo at the beach in swimwear). Others worried about Islamophobic threats, some pertaining to their physical safety, when interacting with strangers online. These situational anxieties as a result of being Muslim-American, coupled with concerns of other Muslim women documented in prior work (e.g., debating whether to share photos of oneself without hijab [53]), left our participants feeling vulnerable.

In addition to the unique context of being a Muslim woman in the U.S., we must also recognize the diversity within the Muslim-American women population compared to populations of women in Muslim-majority countries [6]. Women in our sample, and across the Muslim-American women population, hail from various ethnic, racial, and socioeconomic backgrounds. These different visible and invisible social identities interact and intersect in many ways, exposing individuals to varying experiences of discrimination, privilege, and acceptance. This broad range of social identities results in very different lived experiences, even among our small sample, which further differs from the more unified set of challenges experienced by those living in more homogeneous Muslim-majority countries.

Examining the experiences of people who live with multiple marginalized identities, like Muslim-American women, enables a deeper understanding of how privacy concerns are rooted in the intersection of identities; such insights may not as readily appear when focusing on a single or few minority characteristics. Crenshaw developed the concept of intersectionality [25], drawing on the work of many before her, as a framework for better understanding the intersections of race and gender. Work since then has discussed the application of intersectionality in HCI research [52, 72, 79, 90]. Women of color in the U.S. are subjected to the ramifications of male superiority and white supremacy among other hegemonic structures. Muslim-American women, more specifically, are regularly exposed to sexism, racism, and religious discrimination [20, 64]. The intersections of oppression mean that Muslim-American women often face prejudice for each of their individual identity characteristics, but also in compounded ways that cannot be untangled. This insight was revealed in conversations with many of our participants, including one who was unsure if the hostile looks she received from strangers was due to her hijab or her visible Blackness, making her further protective of both identities.

Our findings add nuance to existing understanding of Islamic norms in the digital world. While Muslim women in Muslim-majority countries face similar religious and cultural expectations within their communities, our participants, as Muslim women in the U.S., described the extra burdens of having to dispel stereotypes to those outside their community, including the 'violent extremist,' the 'oppressed Muslim woman,' and other stereotypes associated with their race, gender, and class identities. The minoritized experience of Muslim-American women helps conceptualize the privacy needs of marginalized Internet users and how they relate to and differ from those of more dominant groups [60].

5.2 Designing for Muslim-American Women

Our findings on the privacy concerns and experiences of Muslim-American women reveal perspectives of individuals living with multiple marginalized identities in relation to privacy, usability, and design. While design improvements alone cannot address deep-rooted structural and cultural issues, we provide some key design insights and opportunities. Our recommendations are closely based on insights provided by our participants and further support prior frameworks for designing usable and useful privacy interfaces [35, 88, 89], social justice-oriented design [28], trauma-informed computing [21], feminist HCI [14], and more. This alignment with prior work indicates the broader benefits of considering—and centering—marginalized users in the design process: as more diverse perspectives are included to better represent the wide spectrum of individuals' privacy needs, users from all backgrounds also stand to benefit from more robust applications of inclusive privacy design.

Considering identity-specific needs. Privacy settings are often difficult to find and use [22, 40]. Our participants echoed this sentiment, and several found privacy settings hard to configure for their goals. While usability issues of privacy settings affect all users, our participants expressed greater insecurity and anxiety due to their identity-specific concerns about consequences of Islamophobia, social surveillance, and more. Participants were particularly frustrated when different platforms had drastically different privacy settings, which posed challenges to their impression and identity management.

Existing guidelines for designing privacy controls often focus on general usability, modality, and legal requirements [35, 88, 103]. Following these principles, making privacy controls easier to find and requiring consistency across platforms might help resolve some of our participants' tensions and provide a stronger sense of safety. As an important next step, usable privacy design needs to shift from solely focusing

on the affordances of privacy controls to also considering how identity and contextual aspects, such as digital literacy skills [35], may affect users' needs. For example, though some design ideologies advocate for less notifications to alleviate burdens on users' cognitive load [83], some of our participants felt extremely anxious about unanticipated system updates and changes to privacy settings due to social surveillance concerns. These participants would benefit from timely and trauma-informed notifications about such changes [21]. Though our participants held many of the same general privacy concerns as other Internet users, the unique contextual factors that affect Muslim-American women must be treated with care and should be reflected in system and interface design.

Enabling identity-based audience controls. Many participants engaged in privacy-protective strategies that were directly tied to their identities as Muslim-American women. For example, some participants were part of closed groups on Facebook or had created private alternatives spaces (e.g., secret accounts under pseudonyms) to share specific content with subgroups of peers. These behaviors allowed our participants to draw clear boundaries and differentiate audiences to cope with context collapse [56], similar to the practices of other marginalized populations such as LGBTQ+ communities [31], sex workers [59], and undocumented immigrants [39].

We suggest that platforms should explore more direct opportunities for users' audience stratification to help users find better channels for peer support and grants users more autonomy. For example, many hijab-wearing participants mentioned a need for women-only digital spaces. Instead of having to go through the tedious process of adding individual users to custom audiences, platforms could offer automatic differentiation options such as 'XYZ trait only' in dropdown lists based on other users' disclosed traits, similar to existing choices like 'friends of friends only' [62]. This type of functionality, however, also presents its own set of challenges. Allowing users to filter others by identity traits could reinforce echo chambers [49] and online segregation [37]. Spaces catering to those who share similar experiences and identities could be abused by predatory individuals for targeted harassment. The feature's design, if not done carefully, could lead to users revealing sensitive characteristics about themselves unintentionally due to the groups they are added to; a potential idea to mitigate this risk is enabling users to only allow particular other users to exercise these filters about them. To avoid misuse and abuse, identity-specific design approaches require further research. Respective guidelines must be crafted carefully in collaboration with community leaders, members, and organizations.

Supporting cross-platform data management. Aside from lists, groups, and audience settings on a particular platform, part of our participants' strategies depended on the ability to curate content and segregate audiences across multiple social media platforms. All participants reported using at least three different platforms, each for distinct purposes. This strategy comes under fire as private companies move towards merging different services and developing integrated ecosystems. For example, Facebook and Instagram, both owned by Meta, are tightly intertwined: Instagram may suggest 'People you may know' based on connections on Facebook, and vice versa [63]. This context collapse creates harms—not just for our participants but also for other marginalized populations [59]—by violating the boundaries users intentionally set to avoid unwanted exposure. Companies should assuage the concerns of these populations by being transparent about how these suggestions are made, and create features that allow them to control if they are suggested to other users, and if yes, to whom.

Providing stronger privacy defaults. Our participants faced repercussions as a result of unexpected default settings on certain platforms. For instance, one participant dealt with reputational damage when family members saw a photo that was unintentionally shared as a result of Facebook's auto-tagging feature. Following this incident, the participant was forced to become more familiar with Facebook's privacy settings and configure them to suit her needs. Prior work suggests that more granular privacy choices can sometimes deter users [51, 95], suggesting the efficiency of improving default options. The instances described by our participants could be avoided by requiring companies to practice privacy by default and set initial privacy settings to be most restrictive (e.g., photo tags requiring user approval). The platform could then ask the user if they want to enable certain features such as auto-tagging, and in doing so, explain both the benefits and potential risks of the feature [89]. This suggestion can come into conflict with the business goals of private-interest companies, and therefore may be better enforced through stronger legislation and regulation.

6 Conclusion

Our findings corroborate with prior Islamic HCI research and show how cultural and religious expectations can be unevenly imposed upon Muslim women [77, 100], and how these expectations shape their practices of navigating online and offline spaces. By focusing on Muslim women living in the U.S., our study contributes new insights into this population's concerns and experiences as they live in societies oriented around Western norms and attitudes. Our participants expressed privacy concerns as a result of being Muslim broadly, as Muslim-American women, and on their individual practice of Islam. Participants adopted countermeasures to make technology work for them, such as developing women-only spaces for self-expression and using Muslim-friendly workplaces to find job postings. Our findings contribute to an intersectional understanding of privacy. We further presented design recommendations for technologies to better cater to the privacy needs of Muslim-American women.

7 Acknowledgements

We thank our community partners and participants for their valuable time and insights. We also thank the anonymous reviewers for their constructive feedback. This research has been partially supported by the Defense Advanced Research Projects Agency (DARPA) under grant No. HR00112010010. The content of the information does not necessarily reflect the position or the policy of the U.S. Government, and no official endorsement should be inferred. Approved for public release; distribution is unlimited.

References

[1] Norah Abokhodair, Adam Hodges, and Sarah Vieweg. Photo sharing in the Arab Gulf: Expressing the collective and autonomous selves. In *ACM Conference on Computer Supported Cooperative Work and Social Computing*, pages 696–711, 2017.

[2] Norah Abokhodair and Sarah Vieweg. Privacy & social media in the context of the Arab Gulf. In *ACM Conference on Designing Interactive Systems*, pages 672–683, 2016.

[3] Alessandro Acquisti, Laura Brandimarte, and George Loewenstein. Privacy and human behavior in the age of information. *Science*, 347(6221):509–514, 2015.

[4] Alessandro Acquisti and Christina Fong. An experiment in hiring discrimination via online social networks. *Management Science*, 66(3):1005–1024, 2020.

[5] Tanisha Afnan, Hawra Rabaan, Kyle ML Jones, and Lynn Dombrowski. Asymmetries in Online Job-Seeking: A Case Study of Muslim-American Women. *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW2):404:1–404:29, 2021.

[6] Sam Afridi. Muslims in America: Identity, Diversity and the Challenge of Understanding, 2001. https://files.eric.ed.gov/fulltext/ED465008.pdf.

[7] Syed Ishtiaque Ahmed, Md Romael Haque, Jay Chen, and Nicola Dell. Digital privacy challenges with shared mobile phone use in Bangladesh. *Proceedings of the ACM on Human-Computer Interaction*, 1(CSCW):17:1–17:20, 2017.

[8] Nader Al Jallad. The concepts of al-halal and al-haram in the Arab-Muslim culture: a translational and lexicographical study. *Language Design: Journal of Theoretical and Experimental Linguistics*, 10(1):77–86, 2008.

[9] Arshad Imtiaz Ali. The impossibility of Muslim citizenship. *Diaspora, Indigenous, and Minority Education*, 11(3):110–116, 2017.

[10] Sajeda Amin. The poverty–purdah trap in rural Bangladesh: implications for women's roles in the family. *Development and Change*, 28(2):213–233, 1997.

[11] Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar, and Erica Turner. Americans and privacy: Concerned, confused and feeling lack of control over their personal information. Technical report, Pew Research Center, 2019.

[12] Imran Awan. Islamophobia and Twitter: A typology of online hate against Muslims on social media. *Policy & Internet*, 6(2):133–150, 2014.

[13] Imran Awan. *Islamophobia in cyberspace: Hate crimes go viral*. Routledge, 2016.

[14] Shaowen Bardzell. Feminist HCI: taking stock and outlining an agenda for design. In *ACM Conference on Human Factors in Computing Systems*, pages 1301–1310, 2010.

[15] Louise Barkhuus. The mismeasurement of privacy: using contextual integrity to reconsider privacy in HCI. In *ACM Conference on Human Factors in Computing Systems*, pages 367–376, 2012.

[16] Timothy Bartkoski, Ellen Lynch, Chelsea Witt, and Cort Rudolph. A meta-analysis of hiring discrimination against Muslims and Arabs. *Personnel Assessment and Decisions*, 4(2):1:1–1:16, 2018.

[17] Johana Bhuiyan. Muslims reel over a prayer app that sold user data: 'a betrayal from within our own community', 2020. https://www.latimes.com/business/technology/story/2020-11-23/muslim-pro-data-location-sales-military-contractors.

[18] 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.

[19] Virginia Braun and Victoria Clarke. Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2):77–101, 2006.

[20] Louis A Cainkar. *Homeland insecurity: the Arab American and Muslim American experience after 9/11*. Russell Sage Foundation, 2009.

[21] 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 *ACM Conference on Human Factors in Computing Systems*, pages 544:1–544:20, 2022.

[22] Yi Chen, Mingming Zha, Nan Zhang, Dandan Xu, Qianqian Zhao, Xuan Feng, Kan Yuan, Fnu Suya, Yuan Tian, Kai Chen, et al. Demystifying hidden privacy settings in mobile apps. In *IEEE Symposium on Security and Privacy*, pages 570–586, 2019.

[23] Danielle Keats Citron and Daniel J Solove. Privacy harms. *SSRN*, 2021. http://dx.doi.org/10.2139/ssrn.3782222.

[24] Juliet Corbin and Anselm Strauss. *Basics of qualitative research: Techniques and procedures for developing grounded theory*. Sage publications, 2014.

[25] Kimberle Crenshaw. Mapping the Margins: Intersectionality, Identity Politics, and Violence against Women of Color. *Stanford Law Review*, 43(6):1241–1299, 1990.

[26] Vanessa P Dennen and Kerry J Burner. Identity, context collapse, and Facebook use in higher education: Putting presence and privacy at odds. *Distance Education*, 38(2):173–192, 2017.

[27] Tamara Dinev, Massimo Bellotto, Paul Hart, Vincenzo Russo, and Ilaria Serra. Internet users' privacy concerns and beliefs about government surveillance: An exploratory study of differences between Italy and the United States. *Journal of Global Information Management*, 14(4):57–93, 2006.

[28] Lynn Dombrowski, Ellie Harmon, and Sarah Fox. Social justice-oriented interaction design: Outlining key design strategies and commitments. In *ACM Conference on Designing Interactive Systems*, pages 656–671, 2016.

[29] Nora A Draper and Joseph Turow. The corporate cultivation of digital resignation. *New Media & Society*, 21(8):1824–1839, 2019.

[30] Rachel Anderson Droogsma. Redefining Hijab: American Muslim women's standpoints on veiling. *Journal of Applied Communication Research*, 35(3):294–319, 2007.

[31] 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.

[32] John L Esposito. *The future of Islam*. Oxford University Press, 2010.

[33] Jennifer C Evans. Hijacking civil liberties: The USA PATRIOT Act of 2001. *Loyola University of Chicago Law Journal*, 33(4):933–990, 2001.

[34] Maha Faisal and Asmaa Alsumait. Social network privacy and trust concerns. In *ACM International Conference on Information Integration and Web-based Applications and Services*, pages 416–419, 2011.

[35] Yuanyuan Feng, Yaxing Yao, and Norman Sadeh. A design space for privacy choices: Towards meaningful privacy control in the internet of things. In *ACM Conference on Human Factors in Computing Systems*, pages 64:1–64:16, 2021.

[36] Batya Friedman, Peter Kahn, and Alan Borning. Value sensitive design: Theory and methods. Technical report, University of Washington, 2002.

[37] Matthew Gentzkow and Jesse M Shapiro. Ideological segregation online and offline. *The Quarterly Journal of Economics*, 126(4):1799–1839, 2011.

[38] Peter Gottschalk and Gabriel Greenberg. From Muhammad to Obama: Caricatures, cartoons, and stereotypes of Muslims. *Islamophobia: The challenge of pluralism in the 21st century*, pages 191–209, 2011.

[39] 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 *ACM Conference on Human Factors in Computing Systems*, pages 114:1–114:15, 2018.

[40] Hana Habib, Sarah Pearman, Jiamin Wang, Yixin Zou, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. "It's a Scavenger Hunt": Usability of Websites' Opt-Out and Data Deletion Choices. In *ACM Conference on Human Factors in Computing Systems*, pages 384:1–384:12, New York, NY, USA, 2020.

[41] Hana Habib, Yixin Zou, Aditi Jannu, Neha Sridhar, Chelse Swoopes, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. An Empirical Analysis of Data Deletion and Opt-Out Choices on 150 Websites. In *Symposium on Usable Privacy and Security*, pages 387–406, 2019.

[42] William Hobbs and Nazita Lajevardi. Effects of divisive political campaigns on the day-to-day segregation of Arab and Muslim Americans. *American Political Science Review*, 113(1):270–276, 2019.

[43] Stefan Huber and Odilo W Huber. The centrality of religiosity scale (CRS). *Religions*, 3(3):710–724, 2012.

[44] Sunny Skye Hughes. US domestic surveillance after 9/11: An analysis of the chilling effect on first amendment rights in cases filed against the Terrorist Surveillance Program. *Canadian Journal of Law and Society*, 27(3):399–425, 2012.

[45] Samia Ibtasam. For God's sake! Considering Religious Beliefs in HCI Research: A Case of Islamic HCI. In *Extended Abstracts of the ACM Conference on Human Factors in Computing Systems*, pages 9:1–9:8, 2021.

[46] Namira Islam. Soft Islamophobia. *Religions*, 9(9):280:1–280:16, 2018.

[47] Amaney Jamal and Nadine Naber. *Race and Arab Americans before and after 9/11: From invisible citizens to visible subjects*. Syracuse University Press, 2008.

[48] Amaney A Jamal. Trump (ing) on Muslim women: The gendered side of Islamophobia. *Journal of Middle East Women's Studies*, 13(3):472–475, 2017.

[49] Kathleen Hall Jamieson and Joseph N Cappella. *Echo Chamber: Rush Limbaugh and the Conservative Media Establishment*. Oxford University Press, 2008.

[50] 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):68–78, 2017.

[51] Stefan Korff and Rainer Böhme. Too much choice: End-user privacy decisions in the context of choice proliferation. In *Symposium On Usable Privacy and Security*, pages 69–87, 2014.

[52] Neha Kumar and Naveena Karusala. Intersectional computing. *Interactions*, 26(2):50–54, 2019.

[53] Rodda Leage and Ivana Chalmers. Degrees of caution: Arab girls unveil on facebook. *Girl wide web*, 2:27–44, 2010.

[54] Douglas Macbeth. On "reflexivity" in qualitative research: Two readings, and a third. *Qualitative Inquiry*, 7(1):35–68, 2001.

[55] Kirsten Martin and Katie Shilton. Why experience matters to privacy: How context-based experience moderates consumer privacy expectations for mobile applications. *Journal of the Association for Information Science and Technology*, 67(8):1871–1882, 2016.

[56] Alice E Marwick and Danah Boyd. I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience. *New Media & Society*, 13(1):114–133, 2011.

[57] Joanna Maselko and Laura D Kubzansky. Gender differences in religious practices, spiritual experiences and health: Results from the US General Social Survey. *Social Science & Medicine*, 62(11):2848–2860, 2006.

[58] Michael E McCullough and Brian LB Willoughby. Religion, self-regulation, and self-control: Associations, explanations, and implications. *Psychological Bulletin*, 135(1):69–93, 2009.

[59] 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 *USENIX Security Symposium*, 2021.

[60] Nora McDonald and Andrea Forte. The Politics of Privacy Theories: Moving from Norms to Vulnerabilities. In *ACM Conference on Human Factors in Computing Systems*, pages 40:1–40:14, 2020.

[61] 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):72:1–72:23, 2019.

[62] Meta. How do I change who can add me as a friend on Facebook?, 2022. https://www.facebook.com/help/217125868312360.

[63] Anna Middleton. How does Instagram know my friends and who to suggest?, 2021. https://www.alphr.com/how-does-instagram-know-friends/.

[64] Heidi Safia Mirza. Embodying the veil: Muslim women and gendered islamophobia in 'new times'. In *Gender, Religion and Education in a Chaotic Postmodern World*, pages 303–316. Springer, 2013.

[65] Travis Mitchell. How Does Pew Research Center Measure the Religious Composition of the US? Answers to Frequently Asked Questions, 2018. https://www.pewresearch.org/religion/2018/07/05/how-does-pew-research-center-measure-the-religious-composition-of-the-u-s-answers-to-frequently-asked-questions/.

[66] Safiek Mokhlis. The effect of religiosity on shopping orientation: an exploratory study in Malaysia. *Journal of American Academy of Business*, 9(1):64–74, 2006.

[67] Alexander Moreira-Almeida, Francisco Lotufo Neto, and Harold G Koenig. Religiousness and mental health: a review. *Brazilian Journal of Psychiatry*, 28(3):242–250, 2006.

[68] Nancy Murray. Profiling in the age of total information awareness. *Race & Class*, 52(2):3–24, 2010.

[69] Maryam Mustafa, Shaimaa Lazem, Ebtisam Alabdulqader, Kentaro Toyama, Sharifa Sultana, Samia Ibtasam, Richard Anderson, and Syed Ishtiaque Ahmed. IslamicHCI: Designing with and within Muslim Populations. In *Extended Abstracts of the ACM Conference on Human Factors in Computing Systems*, pages 20:1–20:8, 2020.

[70] Arvind Narayanan, Arunesh Mathur, Marshini Chetty, and Mihir Kshirsagar. Dark patterns: Past, present, and future: The evolution of tricky user interfaces. *Queue*, 18(2):67–92, 2020.

[71] Helen Nissenbaum. *Privacy in context*. Stanford University Press, 2009.

[72] Ihudiya Finda Ogbonnaya-Ogburu, Angela DR Smith, Alexandra To, and Kentaro Toyama. Critical race theory for HCI. In *ACM Conference on Human Factors in Computing Systems*, pages 265:1–265:16, 2020.

[73] Teresa Valerio Parrot and Stacia Tipton. Using social media "smartly" in the admissions process. *College and University*, 86(1):51–53, 2010.

[74] Sharon K Parsons, Peter L Cruise, Walisa M Davenport, and Vanessa Jones. Religious beliefs, practices and treatment adherence among individuals with HIV in the southern United States. *AIDS Patient Care & STDs*, 20(2):97–111, 2006.

[75] Paul A Pavlou. State of the information privacy literature: Where are we now and where should we go? *MIS Quarterly*, pages 977–988, 2011.

[76] Barbara Perry. Gendered Islamophobia: hate crime against Muslim women. *Social Identities*, 20(1):74–89, 2014.

[77] Hawra Rabaan, Alyson L Young, and Lynn Dombrowski. Daughters of men: Saudi women's sociotechnical agency practices in addressing domestic abuse. *Proceedings of the ACM on Human-Computer Interaction*, 4(CSCW3):224:1–224:31, 2021.

[78] Angel Rabasa, Cheryl Benard, Lowell H Schwartz, and Peter Sickle. *Building moderate Muslim networks*. Rand Corporation, 2007.

[79] Yolanda A Rankin, Jakita O Thomas, and Nicole M Joseph. Intersectionality in HCI: Lost in translation. *Interactions*, 27(5):68–71, 2020.

[80] Mohammad Rashidujjaman Rifat, Mahiratul Jannat, Mahdi Nasrullah Al-Ameen, SM Taiabul Haque, Muhammad Ashad Kabir, and Syed Ishtiaque Ahmed. Purdah, Amanah, and Gheebat: Understanding Privacy in Bangladeshi "pious" Muslim Communities. In *ACM Conference on Computing and Sustainable Societies*, pages 199–214, 2021.

[81] Mohammad Rashidujjaman Rifat, Toha Toriq, and Syed Ishtiaque Ahmed. Religion and Sustainability: Lessons of Sustainable Computing from Islamic Religious Communities. *Proceedings of the ACM on Human-Computer Interaction*, 4(CSCW2):128:1–128:32, 2020.

[82] Dana Rotman, Sarah Vieweg, Sarita Yardi, Ed Chi, Jenny Preece, Ben Shneiderman, Peter Pirolli, and Tom Glaisyer. From slacktivism to activism: participatory culture in the age of social media. In *Extended Abstracts of the ACM Conference on Human Factors in Computing Systems*, pages 819–822, 2011.

[83] Manuel Rudolph, Denis Feth, and Svenja Polst. Why users ignore privacy policies–a survey and intention model for explaining user privacy behavior. In *International Conference on Human-Computer Interaction*, pages 587–598. Springer, 2018.

[84] Johnny Saldaña. *The Coding Manual for Qualitative Researchers*. Sage, 2021.

[85] M Angela Sasse, Matthew Smith, Cormac Herley, Heather Lipford, and Kami Vaniea. Debunking security-usability tradeoff myths. *IEEE Security & Privacy*, 14(5):33–39, 2016.

[86] Jeremy Scahill and Glenn Greenwald. The NSA's secret role in the US assassination program, 2014. https://theintercept.com/2014/02/10/the-nsas-secret-role/.

[87] Christina Scharff. Disarticulating feminism: Individualization, neoliberalism and the othering of 'Muslim women'. *European Journal of Women's Studies*, 18(2):119–134, 2011.

[88] Florian Schaub, Rebecca Balebako, Adam L Durity, and Lorrie Faith Cranor. A design space for effective privacy notices. In *Symposium on Usable Privacy and Security*, pages 1–17, 2015.

[89] Florian Schaub and Lorrie Faith Cranor. Usable and useful privacy interfaces. In Travis D Breaux, editor, *An Introduction to Privacy for Technology Professionals*, pages 176–238. International Association of Privacy Professionals, 2020.

[90] Ari Schlesinger, W Keith Edwards, and Rebecca E Grinter. Intersectional HCI: Engaging identity through gender, race, and class. In *ACM Conference on Human Factors in Computing Systems*, pages 5412–5427, 2017.

[91] Tahseen Shams. Visibility as resistance by Muslim Americans in a surveillance and security atmosphere. *Sociological Forum*, 33(1):73–94, 2018.

[92] Dawinder S Sidhu. The Chilling Effect of Government Surveillance Programs on the Use of the Internet by Muslim-Americans. *University of Maryland Law Journal of Race, Religion, Gender and Class*, 7(2):375–394, 2007.

[93] Andrew Silke. *Routledge handbook of terrorism and counterterrorism*. Routledge, 2019.

[94] Derek MD Silva. The othering of Muslims: Discourses of radicalization in the New York Times, 1969–2014. *Sociological Forum*, 32(1):138–161, 2017.

[95] Daniel Smullen, Yuanyuan Feng, Shikun Aerin Zhang, and Norman Sadeh. The best of both worlds: Mitigating trade-offs between accuracy and user burden in capturing mobile app privacy preferences. *Proceedings on Privacy Enhancing Technologies*, 2020(1):195–215, 2020.

[96] Peter Snyder, Periwinkle Doerfler, Chris Kanich, and Damon McCoy. Fifteen minutes of unwanted fame: Detecting and characterizing doxing. In *ACM Internet Measurement Conference*, pages 432–444, 2017.

[97] Sharifa Sultana, François Guimbretière, Phoebe Sengers, and Nicola Dell. Design Within a Patriarchal Society: Opportunities and Challenges in Designing for Rural Women in Bangladesh. In *ACM Conference on Human Factors in Computing Systems*, pages 536:1–536:13, 2018.

[98] Joseph Turow and Michael Hennessy. Internet privacy and institutional trust: insights from a national survey. *New Media & Society*, 9(2):300–318, 2007.

[99] Margaretha A Van Es. Muslim women as 'ambassadors' of Islam: Breaking stereotypes in everyday life. *Identities*, 26(4):375–392, 2019.

[100] Sarah Vieweg and Adam Hodges. Surveillance & modesty on social media: How Qataris navigate modernity and maintain tradition. In *ACM Conference on Computer-Supported Cooperative Work & Social Computing*, pages 527–538, 2016.

[101] Jessica Vitak. The impact of context collapse and privacy on social network site disclosures. *Journal of Broadcasting & Electronic Media*, 56(4):451–470, 2012.

[102] Michael Wallace, Bradley RE Wright, and Allen Hyde. Religious affiliation and hiring discrimination in the american south: A field experiment. *Social Currents*, 1(2):189–207, 2014.

[103] Na Wang, Heng Xu, and Jens Grossklags. Third-party apps on Facebook: privacy and the illusion of control. In *ACM Symposium on Computer Human Interaction for Management of Information Technology*, pages 4:1–4:10, 2011.

[104] Nina Wang, Allison McDonald, Daniel Bateyko, and Emily Tucker. American dragnet: Data-driven deportation in the 21st century. Technical report, Center on Privacy & Technology at Georgetown Law, 2022.

[105] Alan F Westin. *Privacy and Freedom*. Scribner, 1967.

[106] Andrew L Whitehead, Samuel L Perry, and Joseph O Baker. Make America Christian again: Christian nationalism and voting for Donald Trump in the 2016 presidential election. *Sociology of Religion*, 79(2):147–171, 2018.

[107] Robert E Wilkes, John J Burnett, and Roy D Howell. On the meaning and measurement of religiosity in consumer research. *Journal of the Academy of Marketing Science*, 14(1):47–56, 1986.

[108] Yue "Jeff" Zhang, Jim Q Chen, and Kuang-Wei Wen. Characteristics of Internet users and their privacy concerns: A comparative study between China and the United States. *Journal of Internet Commerce*, 1(2):1–16, 2002.

[109] Shoshana Zuboff. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. Profile books, 2019.

A Pre-Study Survey

1. In which year were you born? Please enter your birth year in 4 digits.

2. I identify my gender as ○ Women ○ Men ○ Non-binary ○ Prefer to self-describe: ___ ○ Prefer not to disclose

3. What is the highest level of education you have completed? ○ Less than high school ○ High school graduate or equivalent ○ Some college ○ Trade, technical or vocational training ○ Associate's degree ○ Bachelor's degree ○ Master's degree ○ Professional degree (JD, MD, etc.) ○ Doctoral degree ○ Other: ___ ○ Prefer not to disclose

4. I identify myself as (please select all that apply): ○ American Indian or Alaska Native ○ Middle Eastern or North African ○ Asian (including South Asian) ○ Hispanic, Latinx, or of Spanish origin ○ Native Hawaiian or Pacific Islander ○ Caucasian ○ Black or African American ○ Other: ___ ○ Prefer not to disclose

5. What is your current employment status? ○ Employed ○ A student ○ A homemaker ○ Military ○ Retired ○ Out of work and looking for work ○ Out of work but not looking for work ○ Other: ___ ○ Prefer not to disclose

6. If you selected "employed" in the previous question, please describe your primary occupation: ___

7. What is your immigration status in the United States? ○ Citizen (born or naturalized) ○ Permanent resident ○ Non-immigrant (student visa, K-1 visa, etc.) ○ Refugee/asylum seeker ○ Other: ___ ○ Prefer not to disclose

8. What is your present religion, if any? ○ Christian (including Protestant, Catholic, etc.) ○ Jewish ○ Muslim (including "Islam, Islamic, Nation of Islam, etc.") ○ Hindu ○ Buddhist ○ No religion, not a believer (including atheist, agnostic) ○ Other: ___ ○ Prefer not to disclose

9. What was your total household income before taxes during the past 12 months? ○ Less than $25,000 ○ $25,000 to $49,999 ○ $50,000 to $74,999 ○ $75,000 to $99,999 ○ $100,000 to $124,999 ○ $125,000 to $149,999 ○ $150,000 or more ○ Prefer not to disclose

10. Do you or anyone in your household own any of the following devices? Please check all that apply. ○ Personal computer ○ Smartphone (can access the Internet, etc.) ○ iPad or other tablet devices ○ E-reader (e.g., Kindle, Nook, etc.) ○ Music Playing Device (e.g., iPod) ○ Console-based gaming system (e.g., Xbox, Nintendo, or Playstation) ○ Voice-activated smart speaker (e.g., Alexa/Echo device, Google Home) ○ Smart TV that connects to the internet ○ Digital media player and microconsole (e.g., Apple TV, Amazon Fire TV) ○ Other: ___ ○ None of the above ○ Prefer not to disclose

11. (For each device selected in the previous question) Thinking about a typical day, how much time do you spend per day using your [Device X]? ○ Never ○ 0-1 hour ○ 1-2 hours ○ 2-3 hours ○ 3-4 hours ○ 4-5 hours ○ 5+ hours ○ I don't know ○ Prefer not to disclose

12. How would you like to be contacted for more information regarding this study? ○ Email (please enter your full email address): ___ ○ Phone (please enter your preferred phone number): ___

B Interview Protocol

Hello, thanks so much for your time and participation today!

I am a PhD student at [anonymized institution], and I'm really interested in understanding the everyday technology practices of Muslim American women, and how technology can be further innovated to best support your needs and leave you feeling empowered. I am also a part of a larger research project at [anonymized institution] who is conducting similar research with other cross cultural populations.

In this interview, we hope to learn how you use technology in your day to day for gathering information and communicating with others, what some of your most pressing questions and concerns are, and how you might feel better supported. We hope to eventually use this research to develop tools to support you and other members of your community in your daily tech practices.

You can expect our conversation to take between an hour and an hour and a half today.

A couple of things before we start:

- We will compensate you $20 for your super valuable time.
- I would like to record this interview to help me remember your responses and later analyze your responses. If you are not comfortable with this conversation being audio or video recorded, please let me know right now.
- To the extent possible, we will ensure that your identity remains completely confidential. This means that we will aggregate comments from all interviews 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 or specific role. If there's anything you really don't want on the record, even if it's anonymous, please let me know that, too.
- This interview is entirely voluntary– if you want to stop the interview at any point during this session, please let me know. We can end the interview at any point and you will still be fully compensated for your time.

Do you have any questions for me? Alright, then let's get started! I'm going to begin the recording and want to confirm that you are consenting to participate in the study.

Part 1: Opening Questions

- On a typical day, what kinds of devices, websites, apps, online services do you usually use? [Probe: Do you own these devices or share them?]
- Are there aspects that concern you when using technology? [Probe: One topic we hear a lot about lately is privacy – to what extent does privacy matter to you if at all?]
- What does 'privacy' mean to you? [Probe: Are there different types of privacy? Does your definition of privacy change when you are online vs. offline?]
- Are you motivated to protect [reiterate what participants said when defining privacy]? Why or why not?

- What 'stuff' do you think about when it comes to privacy risks? What specific things would you want to protect? [Probe: Information about yourself? Certain kinds of information? Information about others in your community or network?]
- Who or what do you need to protect these things from? Who or what poses a risk to your information?
- Are there groups of people who have to worry about protecting their information more than others? [Probe: Yourself? Other members in your community? Muslim-American women in general? Why does this group/person have to worry about it more than others?]

Faith-Related Questions

- What do you think it means to be a Muslim-American woman today? [Probe: How would you describe yourself? Your identity? What's part of that?]
- Are there any experiences unique to being Muslim-American woman today? [Probe: Are there any experiences you would identify as collective experiences for all Muslim-American women?]
- People practice their religion in many different ways. How often do you do something related to practicing your religion? What kinds of things? [Probe: How long have you practiced this way? Have you always practiced this way? Are there times you present as Muslim and other times you do not? How about in online spaces? Do you attend or visit any mosques or religious community centers?]

Part 2: Scenario-Specific Privacy Concerns

Perfect! Thank you for those answers, we're going to be moving on to the next section of our interview now. These next questions are going to be less general and more specific to a couple of different contexts.

Scenario: Ad Tracking

Today it is possible to take personal data about people from many different sources – such as their purchasing and credit histories, their online browsing or search behaviors, or their public records – and combine them together to create detailed profiles of people's potential interests and characteristics. Companies and other organizations use these profiles to offer targeted advertisements or special deals, or to assess how risky people might be as customers.

- Is this something you've already heard about? [Probe: How many companies do you think use profiles like this for their own goals? Would private companies or organizations use this information for any other reasons [than the ones mentioned in blurb]?]
- When you are online, do you ever see advertisements that look like they might be based on a profile of you that uses your personal data?
- What information do you think is used to create these profiles? [Probe: Personal information (e.g., social identities)? Posts on social media? Search terms? Purchases online? Private conversations via text? Can location data from your personal phone's location services be used for these profiles? Is this a good or bad thing?]
- Is there any information about you that might be used for these profiles that you wouldn't want to be used? (E.g., health data, religion, sexual orientation)? Why?
- How accurately do these advertisements actually reflect your interests and personal characteristics?
- How might private companies use a data profile of you in ways that you find acceptable? [Probe: Share your info w/ outside groups doing research that might help improve society? Develop new products? Optimize functionality of the service? Tailor product recommendations?]
- How might private companies use a data profile of you in ways that you find unacceptable? [Probe: What are some concerns you might have about the data private companies are collecting about you?]
- How much control do you feel you have with regards to the information private companies collect about you?

Scenario: US Government/Military Threats

- Based on what you know, do you think what you do (including on your cell phone or offline) is being monitored by the US government or military? How much? Why? [Probe: Does your understanding of what information might be collected about you by the US government or military change the things you do or how you act online?]
- What information do you think the US government or military is particularly interested in collecting about individuals? Why? [Probe: Are they interested in collecting information about some individuals/communities more than others? Why?]
- Do you believe the government collects data about all Americans to assess who might be a potential terrorist threat? [Probe: Is this an acceptable or unacceptable practice? Why or why not? Are some individuals more likely to be monitored closely than others? Why or why not?]
- Do you have any concerns about what information is being collected about you by the US government or military? [Probe: Are any of these concerns related to your identity as a Muslim-American?]

- Have you heard of any instances in which information about people from your community (at large) was collected or used by the US government or military in a way that was harmful?
- Do you think it's possible to go about your daily life without having any government or military entity collect data about you?
- How much control do you feel you have with regards to the information the US government or military collects about you?

Scenario: Online Islamophobia

- Do you think information you share online can be used against you by people you don't know? How?
- Do you think information you share online can be used against you in discriminatory ways? How? [Probe: What kind of information can be used to harm you? What kind of people might want to use information about you to harm you? How might they access that information about you? Do you do anything to protect your information from people you don't know?]
- What platforms or spaces do you feel are people most likely to engage with you in harmful ways? [Probe: Why do you feel this way?]
- Have you ever witnessed or seen an instance of Islamophobia online? [Probe: Would you mind describing that experience?]
- Have you ever personally experienced an instance of Islamophobia online? [Probe: If yes, would you mind describing that experience? If not, have any of your family or friends ever experienced an instance of Islamophobia online?]
- Have you experienced a situation in which what you did online affected your life outside of that space? [Probe: Can your online presence or behavior give rise to discrimination in other environments?]
- How much control do you feel you have over the information you share publicly online with everyone?

Scenario: Social Surveillance & Social Media Use

- What social media platforms or social networking sites do you typically use?
- What kind of information do you share [on mentioned platforms]? Can you give me an example?
- Have you ever hesitated to share something online, even if you weren't posting it publicly? Why?
- What kinds of considerations do you have when posting or sharing something on your personal social media? [Probe: Why do you have these considerations? Does the type of content matter (e.g., political opinions, photos of you, sharing personal thoughts and reflections)? Why or why not? Does the particular social media platform matter? Why or why not?]
- Do you share everything you post online with all of your connections on a given platform? [Probe: Do you have specific audiences that you share specific content with? Do you have specific platforms you share specific content on?]
- Recall a time when you posted something on [particular platform] that you only shared with some of your connections. Can you walk me through the thought process you had as you went through with posting it? [Probe: What would happen if the people you didn't want to share that post with happened to see it?]
- Do you think there can be social consequences to posting certain kinds of content online with your online connections? What are they? [Probe: Where do those consequences come from? Are these consequences related to your identity as a Muslim woman? How? Are these consequences different for Muslim women than they are for Muslim men?]
- We talked about what might be problematic to post/share online. In your practice of your faith, how would you define 'haram' behaviors? [Probe: Is this definition different from how others in your community might describe it? In what ways?]
- Are there similar considerations you have with regards to any other online behaviors (e.g., who you follow, who you are friends with, what you 'like')?
- How much control do you feel you have over the information you share privately online with your connections?

Are there any other important concerns or considerations you have when using the Internet that we have not discussed yet today? Are any of these concerns related to your identity as a Muslim-American woman?

Part 3: Privacy Mitigation Behavior

Now we're going to move away from those context specific questions and think more broadly about all the different concerns we've discussed today.

- I was wondering if you have changed the way you use technology in response to any of those concerns? (E.g., changed settings, used a browser extension/software/other protective tool, abstained from

certain tech usage, etc.) [Probe: Can you tell me about a recent time when you avoided using a specific technology or platform, if that happened? Are there any topics you deliberately choose not to discuss or share via tech (messaging apps, social networks, devices etc.)?]

- Have there been any events in your own life that made you change your technology practices? [Probe: Can you tell me about any specific instances? Is this an active change?]
- Have there been any events related to your identity as a Muslim women broadly that made you change your technology practices? [Probe: Can you tell me about any specific instances? Are you still doing it now?]
- Have you ever experienced a privacy violation, breach, or other negative experience (related to privacy) online? [Probe: For instance, someone gained unwanted access to your personal information?]
- In general, what specific steps, actions or strategies have you taken to protect your personal information and privacy online? Could you give me any specific examples? [Probe: Where or from whom did you learn that strategy? Are these strategies easy or difficult for you to use?]
- What sources do you trust when seeking privacy advice?
- When it comes to protecting your information [or privacy] how helpful or hurtful are the [features/options/settings] on the different apps and platforms you use? [Probe: How could they be better for your needs?]
- How much do you feel you understand the laws and regulations that are currently in place to protect your data privacy?

Part 4: Closing Questions

In your opinion, what are some ways Muslim American women like yourself could better protect themselves online? What seems to be missing for you? (E.g. better tools to allow people to control their personal information, stronger laws regulating what companies can and cannot do with people's personal information, privacy laws and policies that are easier for people to understand and engage with, better/free educational opportunities that teach individuals about online defense tools and strategies)?

Would you be interested in being contacted for future studies? What would be the best way to reach you?

Any questions about our study or any of the topics we discussed today? If you have any questions later you can always contact me at [anonymized email address].

Thank you so much for participating! As we wrap up and I still have you on the line, I'm going to go ahead and send you the virtual gift card and make sure you received it. While I'm doing that, I'm just going to send you a link to this last post-interview survey that's super brief and you can go ahead and leave whenever you're done. [Link]

C Post-Study Survey

1. How often do you think about religious issues? ○ Never ○ Rarely ○ Occasionally ○ Often ○ Very often
2. To what extent do you believe that Allah or something divine exists? ○ Not at all ○ Not very much ○ Neutral ○ Somewhat ○ Very much
3. How often do you take part in religious services? ○ Never ○ Rarely ○ Occasionally ○ Often ○ Very often
4. How often do you experience situations in which you have the feeling that Allah or something divine allows for an intervention in your life? ○ Never ○ Rarely ○ Occasionally ○ Often ○ Very often
5. People practice their religion in different ways. How often, if at all, do you pray? ○ Hardly ever, only during religious holidays ○ Only on Fridays ○ Only on Fridays and religious holidays ○ More than once a week ○ Every day at least once ○ Every day five times
6. How important is religion in your life? ○ Not at all important ○ Not too important ○ Somewhat important ○ Very important