"Like Lesbians Walking the Perimeter": Experiences of U.S. LGBTQ+ Folks With Online Security, Safety, and Privacy Advice

Christine Geeng
University of Washington

Mike Harris
University of Washington

Elissa Redmiles
Max Planck Institute for Software Systems

Franziska Roesner
University of Washington

Abstract

Given stigma and threats surrounding being gay or transgender, LGBTQ+ folks often seek support and information on navigating identity and personal (digital and physical) safety. While prior research on digital security advice focused on a general population and general advice, our work focuses on queer security, safety, and privacy advice-seeking to determine population-specific needs and takeaways for broader advice research. We conducted qualitative semi-structured interviews with 14 queer participants diverse across race, age, gender, sexuality, and socioeconomic status. We find that participants turn to their trusted queer support groups for advice, since they often experienced similar threats. We also document reasons that participants sometimes reject advice, including that it would interfere with their material livelihood and their potential to connect with others. Given our results, we recommend that queer-specific and general security and safety advice focus on specificity—why and how—over consistency, because advice cannot be one-size-fits-all. We also discuss the value of intersectionality as a framework for understanding vulnerability to harms in security research, since our participants' overlapping identities affected their threat models and advice perception.

1 Introduction

About 80% of American *LGBTQ+* (an umbrella acronym including lesbian, gay, bisexual, transgender, and queer) adults use social media sites [98], including for dating and connecting with loved ones. Due to the stigma attached to LGBTQ+ or queer (hereafter used interchangeably) identity, particularly for transgender and non-binary individuals, social media and the web at large can be a safety net to combat alienation [64, 92, 49], but also be a place of significant potential harm [92, 46, 100]. In this paper, and in line with prior work [86, 41], we are interested in potential harms broadly, rather than distinguishing between security, safety, and/or privacy.

Facing such risks online, an individual might seek out advice from a variety of sources. Where does this advice come from, and is it effective? While these questions have been previously studied for *general* security and privacy advice for general populations [85, 87, 89, 88, 43, 90], LGBTQ+ individuals face identity-based risks that straight and cisgender individuals do not [69, 38, 73]. Given prior work suggesting that prioritization increases advice adoption and efficacy, we look to prioritizing and tailoring advice to specific threat models. In this work, we evaluate participants' experiences with advice targeted at queer-specific threat models rather than general online risks.

Our research questions are:

1. Where do queer individuals in the U.S. learn about mechanisms for supporting their online security, safety, and/or privacy?
2. What barriers prevent advice from being effective for queer individuals?
3. How do multiple facets of identity impact queer individuals searching, acting on, or rejecting online security, safety, and/or privacy advice?

To answer our research questions, we conducted qualitative semi-structured interviews with a diverse group of 14 queer individuals. We intentionally recruited for differences across age, race, gender, sexuality, and socioeconomic status so that we could take an intersectional approach to data analysis, as "people's lives... are better understood as being shaped not by a single axis of social division, be it race or gender or class, but by many axes that work together and influence each other" [22].

Our major findings include:

1. Participants often turn to **queer support groups** for advice and **emotional support**, in addition to other

sources like family or work. These support groups serve both to provide individual advice as well as to collectively combat community-level threats. In one example, Participant 14 described her lesbian social media group blocking trolls together "like lesbians walking the perimeter" of their online community.

2. In addition to thinking of time spent or convenience as a trade-off for adopting security advice, participants also lamented **loss of business or joy of connecting with others** as reasons to not adopt privacy practices on social media.

3. **Interlocking facets of identity** affect people's perception and adoption of advice, and participants sometimes prioritize non-queer identity related threats.

Based on our results, we develop takeaways for better security, safety, and privacy advice, with conclusions likely applicable to other vulnerable or marginalized populations as well. For example, we observe that specificity is more important than consistency for advice, since even people with a common identity (e.g., queer) may differ in their threat models (e.g., social media business-user who needs a public profile) and circumstances. As such, we also touch on how intersectionality can be useful, even necessary, in security research when threat modeling. Finally, we stress that advice is limited in preventing harms by placing responsibility of safety on an individual rather than on an institution.

2 Related Work

Our work is motivated by how stigma creates queer-specific threats and vulnerabilities, both offline and online. We also consider how other overlapping identities play a role in risk by discussing research with other vulnerable or marginalized populations. Finally, we summarize prior research on general security advice and targeted advice.

2.1 Queer-Specific Risks

The specific harms and threats that queer folks face (off- and online) due to stigma around sexual orientation or gender have been well-documented.

Technology-independent risks. Risks to queer folks exist independent of technology (e.g., at school, home, and work). Queer youth are more likely than their heterosexual and cisgender (or cis) counterparts to be bullied, consider suicide [5], and be homeless [9]. LGBT youth are often homeless because they are thrown out by their parents upon learning they are gay [9]. While U.S. law technically protects LGBTQ+ people in the workplace [71], in practice their jobs may still be at risk (e.g., a teacher was reportedly fired for being gay after a student discovered his OKCupid profile [2]).

Transgender (or trans) folks, particularly Black or Latino trans women, are disproportionately likely to face violence [13]. Trans/gay panic, a legal defense for someone to justify violence against someone after finding out they are transgender or queer, is still legal in 35 states [7].

Risks on social media. The risks of being out—public about one's identity as queer—indicate how important it is for queer folks to be able to control access to their information. Prior work has noted queer individuals do not always feel safe presenting their queer identity to all audiences on social media [23, 38, 28, 47, 92], a problem more generally known as context collapse [75]. This can be especially stressful for transgender individuals navigating transitioning and coming out on social media [52, 84, 53]. To manage different audiences, individuals use affordances including multiple social media sites or accounts, private accounts, and granular post visibility [38, 28, 47].

Risks in online dating and sexting. Over half of lesbian, gay or bisexual American adults have used a dating app [16]. Online dating can provide queer individuals connection [99] and a space to explore one's identity [38]. It is also a site of privacy tensions, as users often provide location data, use it to connect with people outside of their known social network, and include more sensitive information in profiles [34]. Recently there have been scams extorting queer dating app users by threatening to out them [6].

Sexting through dating apps or through other messaging apps has become a common practice in the U.S. [61], and researchers have highlighted its positive role in relationship satisfaction [27, 40, 96]. Sexting also comes with risks, such as non-consensual sharing of intimate images, that have worse consequences for women and non-binary individuals [48, 68].

Other risks. The prior sections are a non-exhaustive list of possible harms targeted towards queer individuals. Queer and trans activists [69], refugees [17], sex workers [76], and other vocations or identities face other specific threats. Given that our paper is focused on advice for queer folks, not threat models, we leave the full spectrum of financial, physical, relational, and emotional harms [93] for different threat models largely to other work. But we also touch on the importance of these overlapping identities in Section 2.2.

2.2 Intersectional Identities

To understand the complexity of why queer folks adopt or reject advice, and their threat models, we use the framework of intersectionality. This posits that oppression and power is better understood as shaped by multiple axes of identity [22], e.g. but not limited to, race, gender, class, sexuality, and disability [36]. Here we define power as agency and access to resources [37], and power dynamics as "differences in ability to take action between parties" [104].

The reason we are explicitly looking at power is because lack of power reduces one's ability to resist, reduce, or prevent harm [104, 19]. And individuals marginalized across multiple identity axes are a bigger target for harm. For example, being a woman raises one's risk of being harassed online, and this risk is higher for queer women and women of color [33].

Intersectionality also helps us analyze "across domains of power" [22]: across interpersonal, cultural, disciplinary, and structural relationships. For example, a queer employee may be fired by their company for being gay (structural and cultural). And a queer person may be abusive to their partner [42] (interpersonal). Harm can come from institutions, as well as from other marginalized individuals [92, 104]. Given this, we are interested in how individuals at certain intersections may not have the same avenues of recourse after a security breach or unsafe experience, and therefore do not adopt certain advice.

2.3 Security for Vulnerable Populations

There has been interest in the security community around understanding the specific needs of different vulnerable or marginalized populations. For example, this includes studying older adults [45], people with visual impairments [60], sex trafficking survivors [31], refugees [94], and journalists [79]. Our present work fits into that space, deepening our understanding of the experiences of queer individuals in trying to respond to their security/safety/privacy concerns. We hypothesize that some of our conclusions are relevant to other marginalized groups as well.

2.4 Security Advice

Advice evaluation. Providing security education to users has often been a takeaway from user studies on people's security concerns and practices, especially for marginalized groups [94, 31]. Researchers have said that good security advice should be *effective, actionable,* and *understandable* [89, 90]. Yet, general security advice online is often inactionable, whether due to the cost-benefit trade-off not being worth it [62, 43], too much advice existing with no prioritization [89, 20], or that "the right advice might change over time with the attack landscape, new technology, and experience" [90]. And security experts and non-experts have differing opinions on what "good" advice is [66].

Sources of advice. Redmiles et al. found that people often turned to their IT or computer science family and friends for security advice, but people with higher socioeconomic status and technical skill tend to take more advice from the workplace rather than from friends and family [87]. Rader et al. pointed out that informal stories between friends and family about security incidents are useful to learning about security behaviors and changing mental models [85].

Advice for specific populations. The safety priorities and contexts of queer individuals may be different from the general population, and therefore warrant different advice, as "people from different under-served groups may have profoundly different needs and challenges for security and privacy" [106]. Even amongst queer individuals, queer life experiences and concerns can be very different [97]. Security advice exists specifically for women [24], gay online dating [4], queer individuals using Instagram [8], and Black Lives Matter protesters [103] to name a few examples. The Reconfigure Network organized security community workshops and found that contrary to popular cybersecurity narratives that users are uninterested in security, their participants demonstrated care and thoughtfulness in both their own and communal privacy practices, and their practices are shaped by privilege and oppression [14]. We follow Reconfigure's epistemological approach (feminist standpoint theory) of looking to users as experts in their own lives, rather than relying on threat models and advice developed by traditional security experts.

3 Methodology

To answer our research questions, we conducted semi-structured qualitative interviews with queer individuals who use social media, dating apps, or apps for sexting. We asked participants what online safety advice they have given and received, as well as their thought processes behind adopting or rejecting advice. We also collated online documents of queer safety advice as prompts and asked participants how they felt about certain advice relevant to their online activities.

3.1 Interview Protocol

We developed an interview script to ask questions about:

Race		Highest Level of School		Household Income		Age	
White	9	Some college credit, no degree	5	Under $20,000	3	18-24 years old	3
Black	4	Associate degree	2	20,001–40,000	4	25-34 years old	4
Asian	2	Bachelor's degree	5	40,001–60,000	2	35-44 years old	3
Latino	1	Master's or other graduate degree	5	60,001–80,000	1	45-54 years old	2
Native American	1			$100,001 or over	2	65-74 years old	2

Table 1: Participant demographics. We report these in aggregate for our set of 14 participants for participant anonymity. Participants sometimes answered more than one option (e.g., race).

P	Gender	Orientation
1	non-binary	bi
2	woman of trans experience	bi
3	female	pansexual
4	transgender man	gay
5	non-binary	demisexual
6	trans girl	mostly sapphic
7	gender non-conforming	queer
8	non-binary	queer
9	cis woman	queer/bisexual
10	male	homosexual, queer
11	cis male	gay
12	female	lesbian
13	transgender	queer
14	female	lesbian

Table 2: Participants self-reported their gender and sexual orientation.

1. What concerns have participants had about online security / safety / privacy related to queerness? Related to other aspects of their identity? Why do they have these concerns?
2. Have participants ever changed their behaviors to deal with these concerns? How or where did they learn to change their behaviors? Have behavior changes ever failed to solve the problem?
3. Have participants given online safety / security / privacy advice to others?
4. What online advice have participants seen but decided was not for them?
5. If people are unconcerned about online safety / security / privacy, what are they resigned to?

The full interview protocol can be found in Appendix 9.1.

Advice Prompts. We also gathered queer safety advice available online as prompts for participants to think about behaviors related to concerns they had (Appendix 9.2). These prompts were collated from ten pages of online search results for "lgbtq online safety advice". Our goal wasn't to systematically evaluate advice: instead it was to probe participants about what it would be like adopting behavior they had either never thought of or didn't have in recent memory. Therefore, not all participants were asked about the same advice, because it wasn't always relevant to them. Some prompt examples include "use 2-factor authentication" and "on a first date, don't meet at home."

Procedure. Interviews were conducted remotely either by phone or by video conferencing program, depending on participant choice. They ranged from 45 to 90 minutes. Participants were compensated with a $30 gift card. Calls were recorded with participant consent. Only audio data was saved; all video was deleted after the interview.

Interviews were transcribed by two researchers to avoid third-party access to interview data, and were anonymized in the transcription process. Quotes used in this paper are paraphrased for clarity and further anonymity.

Ethics. Due to the potentially harmful memories our interview questions could bring up, we took care to follow best practices from trauma-aware research. We emphasized to participants that they could skip any question and end the interview at any time and still receive compensation. The interviewer listened without judgement and offered participants time to take a moment if needed following a sensitive disclosure. The interviewer also had the Trevor Project hotline number available in case a participant needed to be directed to a counselor (though no participant used the number). We also followed best practices to ethically conduct research with marginalized populations [105], including providing fair compensation and sending the research output (e.g., the paper) to participants after publication. Our study was approved by the University of Washington IRB.

3.2 Participants

We recruited 14 queer participants diverse across age, race, disability, and economic and educational status (Table 1). We determined saturation at 14 participants after no new higher-level themes emerged from the data

and at which point we no longer needed to refine themes after subsequent interviews. Their self-reported gender and sexuality are in Table 2. Participants were recruited through flyers around a major city in the U.S., as well as through postings in queer listservs and other online communities. We also collected demographic information on community type since prior research has shown that queer folks in rural environments face unique concerns [50]. Ten participants live in urban areas, three in suburban areas, and one in a rural area.

3.3 Data Analysis

We conducted thematic analysis on the transcripts, using primarily inductive coding [26]. First, two independent coders familiarized themselves with all transcripts [25]. Then they independently coded four interviews before discussing code choices and agreeing on an intermediate codebook. During the discussion process, they began deductively coding using threat modeling as a framework to include threats and mitigation behaviors as lower-level codes, to be integrated into higher-level themes. They doubled-coded eight more interviews, stopping every two interviews to discuss changes to the codes and higher level themes, until consensus was reached. All transcripts were recoded as necessary. One coder coded the final two interviews.

Inter-rater reliability (IRR) was not calculated because our research goal is the richness and nuance of different experiences, not counts of how often a theme occurred, and because we double-coded and reached consensus on nearly all transcripts [78].

3.4 Author Positionality

Our work is undergirded by feminist standpoint theory, which calls for an understanding that social knowledge and experiences are situated in a specific context [56, 95]. Therefore, we emphasize that the narrative of our results is influenced by our own perspectives and backgrounds. Some authors identify as queer or non-binary and others identify as straight and cis. The authors are either East Asian or white. From an intersectional framework, we recognize that some of us are marginalized across some axes of identity and not others, and that our identities do not fully reflect those of our participants.

4 Results

To provide context for our results, we begin by briefly summarizing key points from participants' threat models. Participants mentioned concerns around homophobic and/or transphobic workplaces, government actors, online strangers, corporations, friends, and family. Some participants were also concerned about harassment from within queer communities. Threats and concerns included, but are not limited to, deadnaming (use of a trans or non-binary person's former name without their consent), transphobic and homophobic harassment, doxxing, losing one's job for being queer, and physical violence.

We now dive into our core research questions, detailing where participants found online safety, security, or privacy information for these threats, their barriers to finding useful advice, and how identity played a role in their advice evaluation.

4.1 Advice Sources

Our participants named a variety of sources from which they either learned something accidentally or they intentionally looked for advice. Purposefully looking for advice was sometimes motivated by a security incident the participant or someone they knew had.

4.1.1 Asking community

Friends and family. Echoing previous work [85, 88], our participants turned to friends and family for safety advice. Some people like P14 mentioned turning to someone in their life who knows tech-related things, in her case her son, who works in IT, for a question on Facebook bans. P1's friends turned to P1 for social media privacy questions because they have a computer security job, even though it is unrelated to social media. Rather than purposely turning to a loved one, P9 learned privacy advice from her partner incidentally. He brought up in casual conversation,

> 'I read online that TikTok is doing such and such things.' I was like that's probably true. But it is a very fun dumb app, so I am going to continue using it.

On the other hand, P11 (cis man, gay) for example, asked a friend with a shared threat model—rather than specific technical expertise—for advice:

> You know, a lot of her concerns [around dating] as a female...I've also learned and realize that this could also be valuable to me as...a queer male.

Queer community. Other participants specifically asked those with whom they shared their queer identity for advice, either because they felt—like P11 with his female friend—that they had a shared identity-based harm or because they had a queer-specific concern. They turned either to their informal queer friend groups or formal queer support groups. For example, at a get-together with

queer friends, P13 gave advice to a friend who wanted to put their "full authentic self" online. Other attendees at the get-together also shared their differing opinions on whether to be more private or public online, creating what P13 described as "kind of a round [table] barbecue."

When P4 (trans man, gay) found a coworker on Grindr and realized they were accidentally outed to each other, and became concerned his workplace would find out, he turned to his trans men support group to hear their experiences and advice on what to do next. As P4 puts it, "It wasn't like we had a leader, but we all just sort of compared notes about what we were doing." Having a group of people to talk to let participants hear about different experiences so they could make an informed decision on what to do next.

For P14 and P12, their Facebook lesbian or LGBTQ+ support groups experienced harassment themselves, and they would turn to in-group members for help.

P6 incidentally came across privacy advice from her queer community, rather than purposely seeking out advice. P6 frequents Twitter and follows other trans and autistic people, some who are very security and privacy conscious. She learned about how to change what gender Twitter assumed she was after seeing a viral tweet about it on her Twitter feed.

Benefit of asking community: emotional support. Getting advice sometimes came with emotional support, which was more common when people sought advice from their trusted community. And it may be especially important right after a harmful event. For example, P12 turned to her queer cousin after getting cyberbullied for posting LGBTQ+ related topics on social media. She described reaching out to her queer cousin as,

> really beneficial. Yeah, I took [the advice] into consideration because I felt I had someone that really cared about me and that really accepted me for who I was.

P14 also took physical privacy advice from his queer community on Tumblr, which previously helped him process and validate his coming out experience with his family. Emotional support helped build trust and gave P14 a place to turn to for future concerns.

When P8 provided advice to an older woman who was worried about sharing a Zoom link publicly, they also worked to calm her fears. P8 said,

> I got this whole Boomer crew that are like, maybe you can teach us [how to Zoom screen share] sometime...And so those are the people who I am both their cheerleader and acknowledge that their fears might have some foundation. To be cautious, but also to embolden them.

Safety concerns and behaviors were tied to emotions, so receiving and providing emotional support was helpful for these participants. P8 stressed the comforting aspect:

> I don't push. I don't push as a practitioner [with] whatever I'm doing with my [yoga] clients, whether it's this kind of [safety concern] conversation or the actual meat of my services. I have to acknowledge where they are.

4.1.2 Learned through vocation or school

For P7, online security was often discussed not just in her home, but also at school or work:

> We literally have to watch like these presentations every year on 'this is why you need to change your password and confidentiality' and blah blah and just keeping unauthorized access at a low.

Redmiles et al. also noted the workplace as a source of digital security advice "in the form of newsletters, IT emails, or required trainings" [88].

P7 learned to change their passwords at least once a year, something they continue to do today, from their high school media technology class. They received a hard drive to save their art and was told to "put your personal password on there to protect it because it's no one else's fault if any of your stuff gets erased." This notion of personal responsibility and concern over art theft, which happened to their friends and almost happened to them, cemented this security behavior. P14, a former teacher, taught her students about how sharing on social media isn't always private: "If you wouldn't want a potential employer to see it in 10 years, you shouldn't be writing it now." And P6 learned about cat-fishing (someone being deceptive in their online dating profile) through a film at her autistic education program.

4.1.3 Searching the web or platform settings

For questions about specific settings, actions, or programs, where the participant already knew the term for what they were looking for, some participants turned to an Internet search engine.

For example, P5 did extensive research on what VPN to use based on their requirement that it not sell their data to third parties. And for advice on dating security and privacy for young women, P3 turned to a YouTube channel run by someone who was previously in an abusive relationship.

P1 was looking for how to change a specific Facebook setting, but only found outdated information that did not apply to their Android phone. P12 looked up how to

Barriers to Finding/Adopting Advice
No language for it
Solution not online
Advice would interfere with income
Advice would interfere with relationships
Distrust in source
Advice out-of-date
Sense of futility

Table 3: Participants mentioned different reasons for not adopting advice.

block someone on Facebook, and someone directed P14 to search Facebook's website for how to block someone, but P14 did not find the site information as helpful as instructions from her friend, who had to block the same person harassing their lesbian Facebook Group.

P8, P11, and P13 mentioned not knowing what language to use to search for certain safety-related information, which will be discussed more below in Section 4.2.1.

4.2 Barriers to Finding and Following Advice

We detail difficulties participants encountered to finding security, safety, and privacy information, as listed in Table 3. While inconvenience was sometimes cited as the reason that advice did not work (as in prior work [62, 88]), our participants faced additional trade-offs as well.

4.2.1 No language for it

P8 and P11 both stated they did not know how to phrase their safety questions to search online, with P8 saying that after having someone duplicate their Instagram account to scam others, "I wouldn't know how to even begin formulating the questions. I'm not even sure what my question would be." During the interview, they said they might search "How do I protect myself?" And P13 said he was not aware that safety advice specifically for queer folks is something that could be found on the Internet.

We note that P8 is in their 40s and started using the Internet in the 90s, P11 is in his 20s, and P13 is in his 60s. Youth and being introduced to the Internet at a young age do not necessarily translate to broad Internet expertise and skills [57].

Some of our participants did bring safety knowledge from one platform to another, but this tended to be analogous experiences of learning to block users on, for example, MySpace and transferring that knowledge to Facebook (P2), or knowledge of Telnet and SMTP's lack of encryption to leading to skepticism of contemporary Internet traffic (P10).

4.2.2 Solution could not be found online

There were a few questions participants had that they could not find answers to. P14 was not sure how a troll's account was still able to harass her on Facebook after she blocked the account. P5 could not find any authoritative source on whether "don't let children talk to adults on the Internet" is reasonable advice (P5 disagreed with this advice because they thought then only predators would talk with children online). P3 tried to learn how to block plastic-surgery related tags which triggered her anxiety on TikTok, but found the app does not have that functionality. And finally, P4 could not find a way to force people to untag his pre-transition photos.

4.2.3 Advice would interfere with material livelihood

As we discuss more below, people's identities are multifaceted. As a result, identity-specific advice to be more cautious online sometimes interferes with their other goals and/or other parts of their identities: for example, participants who also relied on social media for work and income.

For example, P4, a writer, made his Facebook account private after a friend had their social media account duplicated. Eventually, he made his account public again:

> [A friend would say] 'It's such a great post, I want to share it,' and I'm a writer, and so I'd be like yeah I wrote this this long thing that I would love for you to share but you can't....It's not that I'm trying to get exposure on my personal profiles, but I'd like to get my name out there and that was counter-intuitive.

P8, who had their Instagram business account duplicated by a scammer, also did not like the advice to make their account private because doing so would harm their business. P10 mentioned giving advice to a friend who is an event promoter, who was trying to deal with unsolicited messages on his promoter social media page. While P10 suggested to make a separate personal page, his friend did not take this advice, which P10 mused was because, "I guess when you do promotions in the gay world, everyone is your friend." One could see the reverse as well, that every friend is a potential event attendee. These examples illustrate how social media use is sometimes tied to income, and ultimately, financial well-being, which limits people's options for dealing with privacy concerns.

4.2.4 Advice would interfere with joy and relationships

Aside from convenience, participants also noted trade-offs of losing human connection and joy as reasons to not adopt certain security or privacy measures, showing the role emotion plays around security concerns [85], as well as in decision-making in general [30]. Participants who were concerned about harassment on social media or threats from online dating considered the trade-off of using more cautious safety behaviors versus missing potential connection with others.

P14, although she had experienced trolls harassing her on Facebook, did not like the idea of making her account private because having a public account allowed her to meet new people: "It was good to be open to new people in a safe way."

Other participants also considered romantic and sexual connections in their decisions. P3 stated that while she found "don't show your face in sexts" to be reasonable advice, she did not follow it for "vanity reasons". P2, a trans woman, is concerned about being vulnerable to a trans or gay panic defense, where someone can excuse assault or murder by blaming the victim's gender identity or sexual orientation for the assailant's actions [7].

At the same time, P2, who is in her 50s, transitioned and made a lot of life changes in the past couple years, and so will "swing for the fences....I'm just gonna try to live before I die....and make up for lost time." For her, that means dating as much as possible. While she does take precautions for her physical safety by deciding to disclose in her online profile that she is trans and tell a friend if she will meet someone, she is "apprehensive of this in terms of communications through social media. I'm expecting a lot of transphobia."

These examples indicate how while folks value their personal safety, they also value joy and connections in their life. Advice and online safety options for queer folks ideally would not decrease their opportunities to have positive relationships with others, particularly since queer stigma already decreases access to relationships. And as other research notes, there are benefits to visibility for queer folks [28].

4.2.5 Distrust in advice source

Some participants mentioned they would not turn to a source or did not trust the advice they saw there. Reasons included that they didn't want to be sold something (echoing [88]), or they didn't trust the source given how the source's interests differed from their users.

For example, P5, when looking for a VPN that did not sell data to third-parties, searched the web for guides that were not trying to market VPNs to them. They ended up relying on a guide created by what they considered a reputable source, like Wired or Technology Review.

P8 expressed a similar sentiment when explaining why they did not search the Internet for what to do after their Instagram account got duplicated: "I think I'm also fearful that I'd be sold something. I have that experience, and I didn't buy anything and nothing bad happened."

Some participants turned to platforms themselves for information on how to manage their privacy or safety. But they did not always trust that the platform would prioritize user interests over their own. P11 stated about Reddit,

> ...there's some mistrust that I have with some of these platforms where I'm like...do they actually want anonymity? Or do they actually want people to be...moving in this direction where like you have a profile and like, they can personalize things for you right? There's more gain for the business, I think, to do that, than there necessarily could be for me.

4.2.6 Advice becoming out-of-date

Some participants had difficulty using the Internet to find up-to-date security information. P1 tried to find how to change a Facebook privacy setting, but could not find updated advice that worked for their new version of Android OS. When searching for how to make his Facebook more secure, P4 found it helpful that the guide he found had additional user comments

> saying like this is outdated. They don't do this anymore. Or, that's not how that technology works, like almost fact checking the people and saying, you know, this little thing you said was inaccurate or...yes thank you so much, you've helped me.

As P3 and Reeder et al. noted, technology constantly changes, so solutions and threats can also change [90].

4.2.7 Sense of futility in adopting behaviors

Finally, a general barrier we observed to adopting advice was a sense of futility, that any actions a person might take would not address the issue they were concerned about.

For example, after their friend got doxxed, P1 (both of them activists) searched for privacy-enhancing behaviors, while their friend thought, "Well, it's all out there now. There's not much I can do". P9 was also concerned about having worse backlash if she tries to take action, like asking a site to take down her personally identifiable information, citing the "Streisand effect": "the phenomenon whereby the attempt to suppress something

only brings more attention or notoriety to it." [11]. This discouraged her from looking for recourse.

Referencing their identities, P2 and P6 both expressed an acceptance that their engaging in social media or online dating is always going to come with some threat of transphobic people, even with their mitigating behaviors. P6, who never uses the word TERF (trans-exclusionary radical feminist) on Twitter so that transphobes don't find her tweet and harass her, notes that one of her tweets did go viral once which led to some exposure to harassers.

> [Some people,] anytime they see trans people existing online they decide to harass them when they show up on their feed....anytime you get to a big enough reach with a tweet, it's kind of inevitable that some shitty people will see it and want to be shitty at you.

P2 gave up trying to report harassers on Facebook, because:

> It seems like people can catch a ban for something, just for calling someone a bigot for example. But if you actually try to report a transphobic comment, they're not going to care.

She instead only blocks people on Facebook (whereas on Twitter she will both block people and report people for transphobia). Similarly, P14 distrusted Facebook for banning her for using a term for underwear, but not banning a poster for homophobic content. This compounded with her distrust when she had blocked a homophobic harasser, but the harasser came back. She blamed Facebook for blocking not working (whether harasser made a second account or got around the block or ban remains unclear).

Our participants are not alone in their sense of futility. Indeed, Hoffman et al. propose that this world view is actually very rational: "privacy cynicism" is a coping mechanism for Internet users dealing with institution-level, often insurmountable, threats [65]. This coping mechanism may also extend to culture-based threats [22], given, as our participants described, that there are many transphobic and homophobic users online, and moderation policies do not always adequately address this. Our participants did react to threats from their immediate social environment, e.g., cyberbullying, which Hoffman et al. notes is where fatalism is least strong. We discuss the necessity of moving responsibility of safety from vulnerable individuals to powerful institutions in Section 5.2.2.

4.3 Identity

While most participants mentioned safety concerns related to their sexual orientation or gender, they also had overlapping and non-overlapping concerns related to other aspects of their identity, such as their race or age. We discuss how these different facets, including gender more in-depth, impact what advice participants seek based on their threats, and impact their perceptions of advice.

Transitioning. Transitioning is the process where one changes one's gender presentation to match one's internal sense of identity. Transitioning while on social media can lead to both stress and support [52], and can result in shifting threat models and security needs.

For P4, who didn't want to publicly transition on Facebook during early 2010s, the process led him to search how to force people to untag him from old pre-transition photos.

> There was either no information or there was no way to do it. So, some of that stuff still exists because those people either no longer use Facebook, or just didn't do it....I wish there had been like here's a step by step guide of how to clean up your social media without deleting your entire account and restarting it. Most places I searched would say just start over.

This reflects prior work indicating that transitioning users either try to remove old photos or change visibility of those photos on Facebook [53].

P1 also experienced this difficulty of trying to get others to untag their old photos. For P5 (non-binary), transitioning and getting top surgery led to them getting less unsolicited messages, as they no longer presented or were perceived as femme.

Parental Responsibility. After P2 transitioned, she took certain actions to protect her son from transphobic harm, reflecting other queer parents considering their children's privacy [23]. She doesn't bring up her son's name online because:

> I just don't want [a] transphobe [to] somehow infiltrate my [Facebook] friends list and then track him down and cause him harm. I don't put the name of the school or anything like that....I would [also] try to make sure I didn't have any identifying information in the background of the [school] photo for example so that they can figure out where it is....That's probably my biggest fear right now, that my son will get bullied or worse, or otherwise, or hurt because of me.

Age. P8 (non-binary, 45-54) also discussed getting unsolicited sexual messages and accepting that risk as part

of navigating the world while feminine-presenting. She added though, "the older I get the more invisible I am."

For P14 (65-74), aging was an accumulation of stressful discrimination, because of her mobility impairment, religion, and sexuality. She did not want to take the time to learn how to make her church's page private after receiving homophobic harassment because, "When you get old enough and lesbian enough, then you try to deal with that kind of stressful stuff as fast as possible and move on."

Gender. Women are more likely to receive online sexual harassment and stalking than men [100]. We previously detailed how some of our participants, when interpreted as femme, received unsolicited messages. And P3, a cis woman, stated she found it harder to find dating safety advice for queer women than for gay men. Future research should study the quantity and quality of advice that is available to queer sub-communities.

Race. Race also affected how people felt about their risks moving through the world, as described above. P9 stated, "I'm a white person, so I've never been afraid of being a white person on the Internet."

P11 was concerned about dating for both his Asian friend and himself, due to the risk of being stereotyped as submissive and someone aggressive attempting to take advantage of them.

> I think being an Asian man that is queer, there's also these fears of being objectified or sexualized and perceived as being submissive.

He also ruminated on his identity and how that might affect how he perceives online dating advice: "It does feel really fear-based and fear-driven, you know, which I think like in Asian culture can be a big thing."

Relationship with the state. Race also impacted opinions on advice related to the police. When asked whether they found the advice of having a police app (an app that will instantly dial the police with the user's location) handy during a date, P10 (biracial, Black and white) said he would never use it because he's been racially profiled in a gay neighborhood. He stated,

> "The police start questioning me about where do I live, am I homeless....[This incident] really ticked me off because, I'm gay, it's the [gay neighborhood], that's supposed to be my community."

P5 (non-binary, autistic) also did not like the advice, citing previous incidents of police acting violently towards queer and/or autistic individuals. P11 stated it could be useful to someone to give them a sense of security, but he would never call the police on a date. P4 (gay, cis man) didn't trust the police to show up and doing anything, because they ignored his friend getting beat up by a hook-up since the friend and hook-up were both men. He said he trusts friends more, similar to P2. Different aspects of their identities affected participant's relationship with the state and with the utility of the police app advice.

Harms within queer communities. Many participants had queer friends they trusted and could turn to, but this coexists with the reality that queer individuals can also harm other queer individuals. Scheuerman et al. found that transgender folks can experience harm online from both outsiders and insiders of a queer community [92].

Examples of peer-to-peer harms included invalidating a specific identity (e.g., bisexuality [104] or non-binary) within a queer space. P5 mentioned that one time they disagreed in a Twitter thread about how to use pronouns.

> I got shouted down by another queer person....I try to stay away from people who are yelling at other queer people.

Advice should specify if the threat model is potential harms from within a community itself or from outside.

5 Discussion and Future Work

We review the implications of our findings for the development of security advice, for security research more broadly, and areas of investigation for future research.

5.1 Takeaways for Better, Inclusive Safety and Security Advice

Here we provide takeaways for how advice can be improved for queer and non-queer folks, both for communicating advice through conversation, or through written documents that contain advice.

5.1.1 Accept there is no one-size-fits all advice

While mitigations can transfer to other contexts, there is not always a universal solution to a threat because people have different values and circumstances in life [39], as well as different threat models. While some behaviors were common and discussed positively (like blocking people who were causing harm), participants differed on other points such as whether to make social media accounts private. Some of our participants did so to avoid information leakage, and others did not because they needed or wanted social exposure. A behavior option that impairs joy or financial stability is not a fair choice.

Specificity is better than consistency. While Reeder et al. noted that it is an issue when advice is inconsistent across multiple sources [90], we suggest that consistency is not, perhaps the most important goal. Instead, specificity—as we describe approaches below—may better enable people to have autonomy in evaluating what advice is most appropriate for their individual situation. Wade et al. also noted this issue of not including validation or reasoning in BLM protestor advice [103]. Furthermore, Reeder et al. noted technology and other factors change over time, so efforts to create fully consistent advice may find themselves quickly outdated [90].

Provide explanations. To achieve specificity, documents should explain the reasoning behind advice, mirroring how in-person questions allow follow-up questions, for example. Providing reasoning can, however, conflict with another prior recommendation for the creation of security advice: *concision*. Our results suggest that concise advice may also not be ideal. P4 and P5 both mentioned researching articles to find the advice they were looking for, and the detailed explanations of how technology could be used increased their trust in the article. And P9, when prompted with the advice "Use a private account," asked for an explanation of why one should do that before she could say it was good advice or not. As Berdan writes about security advice for journalists, "good advice is rarely a punchy soundbite" [20].

While adding "hows" and "whys" will lengthen documents, advice could be shortened by focusing on a specific threat to mitigate. For example, rather than writing a general online safety advice list for queer folks, a document could focus on a specific platform (e.g. Grindr [4], Instagram [8]), activity (e.g. transitioning, activism), or threat (e.g., being outed to family and friends, community in-fighting, extortion scams on queer dating apps [6]). Advice could be tailored towards platform novices or platform experts, especially given prior work suggesting differences in protective behavior amongst those with different levels of digital skill [58, 32].

5.1.2 Share emotional and communal support with advice

Communication research has pointed out that advice preceded by emotional support was considered higher quality [44]. Security clinic professionals provide emotional support as part-and-parcel of their service [101], which is necessary for clients facing intimate partner violence [102]. In community security workshops, relieving anxiety and making sure participants feel in control of their lives is an important part of the security teaching/learning process [14]. While our work cannot discern whether or not participants were more likely to accept advice when it came with emotional support, several of our participants did seek it out, and P12 spoke positively when the friend she turned to after a cyber-bullying incident provided it.

Further, P4 discussed how his trans men support group would "compare notes about what we were doing" when providing advice. He was looking for information on whether to delete his old account prior to his transition or to just untag all photos, and people in his group described their experience doing different things before P4 made his decision. (He opted to untag photos so he wouldn't get questions about why his Facebook account was so new.) Thus, his group was engaged in collaborative advice giving, perhaps leading to group members feeling less alone in their struggles.

Support security workshops and existing support groups. Given how our results indicate the benefit of support groups as a space to ask questions and share experiences, as well as provide emotional support, safety advice may be better discussed in a group setting. As Slupska et al. writes, "Cybersecurity is more effective when it is communal...Discuss[ing] online threats and mitigations with members of a community makes it easier and less intimidating to take action."

This can look like security researchers hosting community workshops, e.g., CryptoHarlem [3], Reconfigure Network, and PEN America [12]. It could also look like security researchers providing resources for existing queer support groups in some fashion. These cybersecurity advocates need to have "people skills", empathy, and respect for user capabilities in order to establish trusting relationships and empower users to believe in their own abilities [54, 55].

Research with other stigmatized groups have also shown the importance of online discussion forums and communities for developing and distributing risk mitigation strategies, such as sex workers [21]. For online settings, creating affordances for collaborative discussion and feedback on advice documents may create better buy-in, sense of emotional support, and ability to archive out-of-date advice. Regardless of the format, it is important that the advice-giver listens to the individual's needs as they are experts in their own lives [14, 95].

5.1.3 Communicate credibility

As prior advice research [89], credibility research [80], and our results show, participants distrusted sites that seemed to market a product. Credible advice should not look like it is selling something. Future work should look at what degree of marketing content that credibility drops off, e.g., a social media site with poor reputation versus a blog with some advertisements.

Also, some participants distrusted privacy instructions on platform sites, since they consider platforms to pri-

oritize business interests over user harm. Therefore it is important for third parties, like the Electronic Frontier Foundation [10], to continue writing advice and instructions on controlling security and privacy settings. At the same time, platforms should still provide instructions for security settings as well, given that participants chose to look there.

5.2 Takeaways for Security Research

5.2.1 Incorporating intersectionality in security research

Our findings with our diverse participants underscore an intersectional understanding of power and threats, which we argue should be considered systematically when threat modeling. Some intersectionality themes relevant to social factors security research include:

1. Someone marginalized across multiple identities may not have the same agency to reduce harm as someone marginalized across one identity [37].

2. Members of one marginalized group can harm another marginalized group. As Collins writes, "Depending on the context, an individual may be an oppressor, a member of an oppressed group, or simultaneously oppressor and oppressed" [63].

3. Oppression (and harm) can come from interpersonal connections, culture, disciplinary structures, or institutions [22], and an individual under threat in one relationship might have agency in a different relationship.

As the security field continues to research specific populations, an intersectional approach will be useful to understand how the threats within one population may differ. Recruiting a diverse set of queer participants was important for us to illustrate how people often had concerns related to multiple axes of identity, e.g., being Asian American and gay. For some, concerns related to another identity were prioritized over their queerness in the moment of the interview. These examples show how in different contexts, one axis of oppression might be more relevant than others, and threat modeling for someone should explore these priorities. We argue that differences are just as important to study and design for as generalities, since there is no universal technology user [35].

These intersectional identities also affected what advice would work or participants could afford to adopt: P8 was not able to make their business Instagram profile private after being harassed due to potential loss of customers, and multiple participants did not trust reporting homophobic and transphobic posts to Facebook because they have seen such posts remain up. The power difference between the individual and adversary affects one's sense of agency in controlling one's safety. Making power imbalances explicit in threat modeling is important to understanding what mitigations an individual is capable of, and when structural changes are necessary.

While this framework surfaces how the queer experience is not a monolith, it also reveals when harm mitigations are transferable to others (which Wang also mentions as a motivation to pursue inclusive security and privacy [106]). For example, Nova et al. recommends that online platforms design group-level blocking functionality, as people of the queer Hijra identity from Bangladesh are "significantly influenced by their group dynamics and largely dependent on the sharing of information within communities" [81]. P14 had difficulty learning to block a harasser in her elder lesbian Facebook group, and could benefit from this affordance. Reichel also notes that low-income South African mobile users rely on blocking rather than Facebook settings for privacy protection [91]. Future work could explore when similar effects of marginalization across different groups can lead to similar threat models, as well as when affordances are common enough across platforms (e.g., blocking) that it can be recommended generally.

5.2.2 Limitations of security advice as personal responsibility

While improving security advice for queer individuals is important, advice as a solution for harms is limited because it places an overwhelming responsibility on an individual [74, 95]. Individual behaviors will not always work because a) the problems folks face may involve other people (e.g., networked privacy [74]), and b) when institutions are the threat, individuals don't have equal resources and power.

Prior research notes that managing security and privacy can be a communal goal [81, 60, 107], and that because privacy is networked, one person's disclosure decisions inevitably affect their entire social circle [75, 74]. And as mentioned earlier, some of P2's privacy behaviors around her being transgender is to protect her son. Advice can be formulated with a community in mind, such as Pen America's online harassment guide for witnesses and allies [12].

Individual or communal advice also has limits when threats are powerful institutions, such as corporations or governments, or culture (e.g., transphobia). The futility some of our participants experienced around online harms are clearer with this context, and moving responsibility of safety to those in power would better address certain threats. Research on problematic content in ads [108], privacy policy unreadability [77], sex worker safety [19], prisoner surveillance [82], undocumented

immigrant surveillance [51], to name a few contexts, all recommend government or platform policy changes to best protect their target users. We support and contribute research to improve safety advice, while also pointing out the necessity of structural changes to make queer lives safer (e.g., banning gay/trans panic defense [7], communal blocking on platforms [1]).

5.3 Future Work

Our work focuses on queer folks in the U.S., but there are other contexts security advice can be analyzed through other than by community or population. Pierce et al. outlined spectrums of security toolkit traits: some toolkits were designed to be used before an incident (preventative) or after (provoked responses), and some were designed to be done once or done regularly (security hygiene) [83]. Future research could look into how security advice meant for regular checkups might work better as a concise checkbox list, particularly for those already familiar with security behaviors, while something communicated after an incident may require more tact and emotional support.

For support groups, we raise the question of when "technical" experts are needed, and what kind of expertise is lacking. If experts are integrated into a group, how do you train an expert to ensure they are suited for their outsider role? Future research can explore collaborating with online support groups to understand how advice gets adopted, as online support groups have been known to provide advice and emotional support for specific communities [15, 76, 18]. Finally, it remains an open question whether seeing conflicting advice lowers users' trust in an advice source.

While we used threat modeling to help organize our results, we did not follow particular information-seeking theories. Health research has differently modeled seeking safety information related to risk, e.g., diseases or natural disasters [29]. Future advice research could incorporate theory outside security, e.g., the planned risk information seeking model [67].

Finally, we ask when is it better to study a specific threat model or platform versus a specific identity when it comes to designing for harm mitigation or educating for harm mitigation.

6 Limitations

This research scratches the surface of queer-intersecting identities that lead to other vulnerabilities (e.g. LGBTQ+ refugees [17], sex workers [72], HIV positive folks [70], victims of intimate partner violence [42], activists [69], and parents [23] as a non-exhaustive list) or different contexts (non-U.S. cultures and nationalities [17, 81]). We provide a foundation for security researchers to think intersectionally when threat modeling and addressing harms when multiple identities play a role in risk.

Our work faces limitations common to qualitative work: we cannot evaluate the popularity of a source or test statistical significance of identity factors on decision-making. We leave this to future work.

We believe our general insights into traits of good advice is transferrable to other contexts [59], but future research is needed to understand when and where specific advice (e.g., "use a private account") works best. Our work also focuses on queer folks generally, including both cisgender and transgender individuals. As noted earlier, transgender individuals face specific vulnerabilities [69], and advice research with transgender folks specifically is also needed.

7 Conclusion

We studied where LGBTQ+ folks in the U.S. turn to for safety, security, and privacy advice because this population faces unique threats from their families, communities, and the state due to homophobia and transphobia. Through qualitative interviews with 14 diverse queer individuals, we found participants turned to queer support groups, whom they trusted and often shared threat models with, for help, in addition to other sources listed in prior security advice work. Participants cited loss of business or joy of connecting with others as reasons to not adopt advice, in addition to inconvenience.

Other aspects of identity like race and age played a role in what threats participants expected and looked to advice for. We recommend that advice favor specificity over consistency because different identities can lead to different threat models. We also argue for using intersectionality to understand how interlocking identities lead to higher risk of harms or constrain what mitigating behaviors people can adopt. We also echo calls for policy and other structural approaches to make marginalized populations safer, rather than only focusing on personal responsibility to find good advice. Finally, our work provides a foundation for understanding how overlapping identity threat models affect advice-seeking.

8 Acknowledgements

We thank our study participants for sharing their perspectives and time with us. We thank Sheamus Heikkila, Tadayoshi Kohno, Naveena Karusala, Lucy Simko, Emily Tseng, and Miranda Wei for their valuable feedback. We thank Seattle AARP and the Reddit moderators of r/gaysian for their help in recruiting participants. This work was supported in part by a gift from Google.

References

[1] Block together is shut down. https://blocktogether.org/. (Accessed on 10/08/2021).

[2] Catholic school teacher reportedly fired after being outed as gay — teen vogue. https://www.teenvogue.com/story/catholic-school-teacher-reportedly-fired-after-outed-as-gay. (Accessed on 10/07/2021).

[3] Cryptoharlem. https://www.cryptoharlem.com/. (Accessed on 09/16/2021).

[4] GRINDR HOLISTIC SECURITY GUIDE. Grindr 4 Equality, https://www.grindr.com/g4e/G4E-HolisticSecurityGuide-English.pdf. (Accessed on 02/07/2021).

[5] Health Disparities Among LGBTQ Youth — Health Disparities — Adolescent and School Health — CDC. https://www.cdc.gov/healthyyouth/disparities/health-disparities-among-lgbtq-youth.htm. (Accessed on 10/07/2021).

[6] How to spot extortion scams on LGBTQ+ dating apps — FTC Consumer Information. FTC, https://www.consumer.ftc.gov/blog/2021/09/how-spot-extortion-scams-lgbtq-dating-apps. (Accessed on 09/17/2021).

[7] Movement Advancement Project — Gay/Trans Panic Defense Bans. https://www.lgbtmap.org/equality-maps/panic_defense_bans. (Accessed on 09/30/2021).

[8] PROTECT YOUR SPACE AND WELL-BEING ON INSTAGRAM. The Trevor Project, https://www.thetrevorproject.org/wp-content/uploads/2019/06/IG-x-Trevor-Project_LGBTQ-Safety-Guide.pdf. (Accessed on 02/07/2021).

[9] Serving Our Youth: Findings from a National Survey of Service Providers Working with Lesbian, Gay, Bisexual, and Transgender Youth who are Homeless or At Risk of Becoming Homeless. Williams Institute, https://williamsinstitute.law.ucla.edu/wp-content/uploads/Serving-Our-Youth-July-2012.pdf. (Accessed on 10/07/2021).

[10] Surveillance self-defense — tips, tools and how-tos for safer online communications. Electronic Frontier Foundation, https://ssd.eff.org/. (Accessed on 10/12/2021).

[11] Words We're Watching: 'Streisand effect' — Merriam-Webster. https://www.merriam-webster.com/words-at-play/words-were-watching-streisand-effect-barbra. (Accessed on 10/02/2021).

[12] Writers at Risk - PEN America. https://pen.org/issue/writers-at-risk/. (Accessed on 09/16/2021).

[13] Dismantling a Culture of Violence: Understanding Anti-Transgender Violence and Ending the Crisis. https://hrc-prod-requests.s3-us-west-2.amazonaws.com/files/assets/resources/Dismantling-a-Culture-of-Violence-010721.pdf, Dec 2020. (Accessed on 10/07/2021).

[14] Reconfigure: Feminist Action Research in Cybersecurity. Oxford Internet Institute, https://www.oii.ox.ac.uk/wp-content/uploads/2021/01/Reconfigure-Report-v6-pages.pdf, Feb 2021.

[15] AMMARI, T., AND SCHOENEBECK, S. Understanding and supporting fathers and fatherhood on social media sites. In *Proceedings of the 33rd annual ACM conference on human factors in computing systems* (2015), pp. 1905–1914.

[16] ANDERSON, M., VOGELS, E. A., AND TURNER, E. Online Dating: The Virtues and Downsides — Pew Research Center. https://www.pewresearch.org/internet/2020/02/06/the-virtues-and-downsides-of-online-dating/. (Accessed on 10/07/2021).

[17] ANDREASSEN, R. Social media surveillance, LGBTQ refugees and asylum. *First Monday* (2021).

[18] BARAKAT, H., AND REDMILES, E. M. Community Under Surveillance: Impacts of Marginalization on an Online Labor Forum. In *16th International AAAI Conference on Web and Social Media* (2021).

[19] BARWULOR, C., MCDONALD, A., HARGITTAI, E., AND REDMILES, E. M. "Disadvantaged in the American-Dominated Internet": Sex, Work, and Technology. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2021), CHI '21, Association for Computing Machinery.

[20] BERDAN, K. An evaluation of online security guides for journalists. https://cltc.berkeley.edu/wp-content/uploads/2021/01/Online_Security_Guides_for_Journalists.pdf.

[21] BERNIER, T., SHAH, A., ROSS, L. E., LOGIE, C. H., SETO, E., ET AL. The use of information and communication technologies by sex workers to manage occupational health and safety: scoping review. *Journal of medical internet research 23*, 6 (2021), e26085.

[22] BILGE, S., AND COLLINS, P. H. Intersectionality. *Cambridge, UK: Polity* (2016).

[23] BLACKWELL, L., HARDY, J., AMMARI, T., VEINOT, T., LAMPE, C., AND SCHOENEBECK, S. LGBT parents and social media: Advocacy, privacy, and disclosure during shifting social movements. In *Proceedings of the 2016 CHI conference on human factors in computing systems* (2016), pp. 610–622.

[24] BLUE, V. *The Smart Girl's Guide to Privacy: Practical Tips for Staying Safe Online*. No Starch Press.

[25] BRAUN, V., AND CLARKE, V. Using thematic analysis in psychology. *Qualitative research in psychology 3*, 2 (2006), 77–101.

[26] BRAUN, V., AND CLARKE, V. Conceptual and design thinking for thematic analysis. *Qualitative Psychology* (2021).

[27] BURKETT, M. Sex (t) talk: A qualitative analysis of young adults' negotiations of the pleasures and perils of sexting. *Sexuality & Culture 19*, 4 (2015), 835–863.

[28] CARRASCO, M., AND KERNE, A. Queer visibility: Supporting LGBT+ selective visibility on social media. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (2018), pp. 1–12.

[29] CASE, D. O., AND GIVEN, L. M. *Looking for information: A survey of research on information seeking, needs, and behavior*. Emerald Group Publishing, 2016.

[30] CHAI, S. *Choosing an identity: A general model of preference and belief formation*. University of Michigan Press, 2001.

[31] CHEN, C., DELL, N., AND ROESNER, F. Computer security and privacy in the interactions between victim service providers and human trafficking survivors. In *28th USENIX Security Symposium (USENIX Security 19)* (2019), pp. 89–104.

[32] CHEN, J., PAIK, M., AND MCCABE, K. Exploring internet security perceptions and practices in urban ghana. In *10th Symposium On Usable Privacy and Security (SOUPS)* (2014), pp. 129–142.

[33] CITRON, D. K. *Hate crimes in cyberspace*. Harvard University Press, 2014.

[34] COBB, C., AND KOHNO, T. How public is my private life? privacy in online dating. In *Proceedings of the 26th International Conference on World Wide Web* (2017), pp. 1231–1240.

[35] COSTANZA-CHOCK, S. *Design justice: Community-led practices to build the worlds we need*. The MIT Press, 2020.

[36] CRENSHAW, K. Demarginalizing the intersection of race and sex: A black feminist critique of antidiscrimination doctrine, feminist theory and antiracist politics. *u. Chi. Legal f.* (1989), 139.

[37] CRENSHAW, K. Mapping the margins: Intersectionality, identity politics, and violence against women of color. *Stan. L. Rev. 43* (1990), 1241.

[38] DEVITO, M. A., WALKER, A. M., AND BIRNHOLTZ, J. 'Too Gay for Facebook' Presenting LGBTQ+ Identity Throughout the Personal Social Media Ecosystem. *Proceedings of the ACM on Human-Computer Interaction 2*, CSCW (2018), 1–23.

[39] DOURISH, P., GRINTER, R. E., DE LA FLOR, J. D., AND JOSEPH, M. Security in the wild: user strategies for managing security as an everyday, practical problem. *Personal and Ubiquitous Computing 8*, 6 (2004), 391–401.

[40] DROUIN, M., COUPE, M., AND TEMPLE, J. R. Is sexting good for your relationship? It depends.... *Computers in Human Behavior 75* (2017), 749–756.

[41] DYM, B., AND FIESLER, C. Social norm vulnerability and its consequences for privacy and safety in an online community. *Proceedings of the ACM on Human-Computer Interaction 4*, CSCW2 (2020), 1–24.

[42] ELLIOT, P. Shattering illusions: Same-sex domestic violence. *Journal of Gay & Lesbian Social Services 4*, 1 (1996), 1–8.

[43] FAGAN, M., AND KHAN, M. M. H. Why do they do what they do?: A study of what motivates users to (not) follow computer security advice. In *Twelfth Symposium on Usable Privacy and Security (SOUPS)* (2016), pp. 59–75.

[44] FENG, B. Testing an integrated model of advice giving in supportive interactions. *Human Communication Research 35*, 1 (2009), 115–129.

[45] FRIK, A., NURGALIEVA, L., BERND, J., LEE, J., SCHAUB, F., AND EGELMAN, S. Privacy and security threat models and mitigation strategies of older adults. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS)* (2019), pp. 21–40.

[46] GAY, L., NETWORK, S. E., ET AL. Out online: The experiences of lesbian, gay, bisexual and transgender youth on the internet. *New York, NY* (2013).

[47] GEENG, C. LGBTQ privacy concerns on social media. In *Proceedings of the 2018 CHI Conference Workshops and Symposia on Human Factors in Computing Systems*, ACM Press.

[48] GEENG, C., HUTSON, J., AND ROESNER, F. Usable sexurity: Studying people's concerns and strategies when sexting. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS)* (2020), pp. 127–144.

[49] GRAY, M. L. Negotiating identities/queering desires: Coming out online and the remediation of the coming-out story. *Journal of Computer-Mediated Communication 14*, 4 (2009), 1162–1189.

[50] GRAY, M. L. *Out in the Country*. New York University Press, 2009.

[51] GUBEREK, T., MCDONALD, A., SIMIONI, S., MHAIDLI, A. H., TOYAMA, K., AND SCHAUB, F. Keeping a Low Profile?: Technology, Risk and Privacy among Undocumented Immigrants. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems - CHI '18*, ACM Press, pp. 1–15.

[52] HAIMSON, O. L., BRUBAKER, J. R., DOMBROWSKI, L., AND HAYES, G. R. Disclosure, Stress, and Support During Gender Transition on Facebook. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing*, ACM, pp. 1176–1190.

[53] HAIMSON, O. L., BRUBAKER, J. R., DOMBROWSKI, L., AND HAYES, G. R. Digital footprints and changing networks during online identity transitions. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (2016), pp. 2895–2907.

[54] HANEY, J. M., AND LUTTERS, W. G. Skills and characteristics of successful cybersecurity advocates. In *Workshop Program at Symposium on Usable Privacy and Security (SOUPS) 2017* (2017).

[55] HANEY, J. M., AND LUTTERS, W. G. "It's Scary...It's Confusing...It's Dull": How Cybersecurity Advocates Overcome Negative Perceptions of Security. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS)* (2018), pp. 411–425.

[56] HARAWAY, D. Situated knowledges: The science question in feminism and the privilege of partial perspective. *Feminist studies 14*, 3 (1988), 575–599.

[57] HARGITTAI, E. Digital na(t)ives? Variation in internet skills and uses among members of the "net generation". *Sociological inquiry 80*, 1 (2010), 92–113.

[58] HARGITTAI, E., ET AL. Facebook privacy settings: Who cares? *First Monday* (2010).

[59] HATCH, J. A. *Doing qualitative research in education settings*. Suny Press, 2002.

[60] HAYES, J., KAUSHIK, S., PRICE, C. E., AND WANG, Y. Cooperative privacy and security: Learning from people with visual impairments and their allies. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS)* (2019).

[61] HERBENICK, D., BOWLING, J., FU, T.-C., DODGE, B., GUERRA-REYES, L., AND SANDERS, S. Sexual diversity in the United States: Results from a nationally representative probability sample of adult women and men. *PloS one 12*, 7 (2017), e0181198.

[62] HERLEY, C. So long, and no thanks for the externalities: The rational rejection of security advice by users. In *Proceedings of the 2009 Workshop on New Security Paradigms Workshop* (New York, NY, USA, 2009), NSPW '09, Association for Computing Machinery, p. 133–144.

[63] HILL COLLINS, P. Black Feminist Thought in the Matrix of Domination. In *Black Feminist Thought: Knowledge, Consciousness, and the Politics of Empowerment*. Routledge, pp. 221–238.

[64] HILLIER, L., MITCHELL, K. J., AND YBARRA, M. L. The Internet as a safety net: Findings from a series of online focus groups with LGB and non-LGB young people in the United States. *Journal of LGBT Youth 9*, 3 (2012), 225–246.

[65] HOFFMANN, C. P., LUTZ, C., AND RANZINI, G. Privacy cynicism: A new approach to the privacy paradox. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace 10*, 4 (2016).

[66] ION, I., REEDER, R., AND CONSOLVO, S. "...No one can hack my mind": Comparing Expert and Non-Expert Security Practices. In *Eleventh Symposium On Usable Privacy and Security (SOUPS)* (2015), pp. 327–346.

[67] KAHLOR, L. Prism: A planned risk information seeking model. *Health communication 25*, 4 (2010), 345–356.

[68] LENHART, A., YBARRA, M., AND PRICE-FEENEY, M. Nonconsensual image sharing: one in 25 Americans has been a victim of "revenge porn". Data & Society Research Institute, 2016.

[69] LERNER, A., HE, H. Y., KAWAKAMI, A., ZEAMER, S. C., AND HOYLE, R. Privacy and activism in the transgender community. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (2020), pp. 1–13.

[70] LIANG, C., HUTSON, J. A., AND KEYES, O. Surveillance, stigma & sociotechnical design for HIV. *First Monday* (2020).

[71] LIPTAK, A. Civil rights law protects gay and transgender workers, Supreme Court rules. *The New York Times 1* (2020).

[72] LYONS, T., KRÜSI, A., PIERRE, L., KERR, T., SMALL, W., AND SHANNON, K. Negotiating violence in the context of transphobia and criminalization: The experiences of trans sex workers in Vancouver, Canada. *Qualitative health research 27*, 2 (2017), 182–190.

[73] MAHOWALD, L., GRUBERG, S., AND HALPIN, J. The State of the LGBTQ Community in 2020 - Center for American Progress. `https://www.americanprogress.org/issues/lgbtq-rights/reports/2020/10/06/491052/state-lgbtq-community-2020/#Ca=10`, Oct 2020.

[74] MARWICK, A., FONTAINE, C., AND BOYD, D. "Nobody sees it, nobody gets mad": Social media, privacy, and personal responsibility among low-SES youth. *Social Media+ Society 3*, 2 (2017), 2056305117710455.

[75] MARWICK, A. E., AND BOYD, D. Networked privacy: How teenagers negotiate context in social media. *New media & society 16*, 7 (2014), 1051–1067.

[76] MCDONALD, A., BARWULOR, C., MAZUREK, M. L., SCHAUB, F., AND REDMILES, E. M. "It's stressful having all these phones": Investigating Sex Workers' Safety Goals, Risks, and Practices Online. In *30th USENIX Security Symposium (USENIX Security 21)* (2021).

[77] MCDONALD, A. M., AND CRANOR, L. F. The cost of reading privacy policies. *Isjlp 4* (2008), 543.

[78] MCDONALD, N., SCHOENEBECK, S., AND FORTE, A. Reliability and inter-rater reliability in qualitative research: Norms and guidelines for CSCW and HCI practice. *Proceedings of the ACM on Human-Computer Interaction 3*, CSCW (2019), 1–23.

[79] MCGREGOR, S. E., CHARTERS, P., HOLLIDAY, T., AND ROESNER, F. Investigating the computer security practices and needs of journalists. In *24th USENIX Security Symposium (USENIX Security 15)* (2015), pp. 399–414.

[80] METZGER, M. J., FLANAGIN, A. J., AND MEDDERS, R. B. Social and heuristic approaches to credibility evaluation online. *Journal of communication 60*, 3 (2010), 413–439.

[81] NOVA, F. F., DEVITO, M. A., SAHA, P., RASHID, K. S., ROY TURZO, S., AFRIN, S., AND GUHA, S. "Facebook Promotes More Harassment" Social Media Ecosystem, Skill and Marginalized Hijra Identity in Bangladesh. *Proceedings of the ACM on Human-Computer Interaction 5*, CSCW1 (2021), 1–35.

[82] OWENS, K., COBB, C., AND CRANOR, L. "You Gotta Watch What You Say": Surveillance of Communication with Incarcerated People. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (2021), pp. 1–18.

[83] PIERCE, J., FOX, S., MERRILL, N., AND WONG, R. Differential vulnerabilities and a diversity of tactics: What toolkits teach us about cybersecurity. *Proceedings of the ACM on Human-Computer Interaction 2*, CSCW (2018), 1–24.

[84] PINTER, A. T., SCHEUERMAN, M. K., AND BRUBAKER, J. R. Entering Doors, Evading Traps: Benefits and Risks of Visibility During Transgender Coming Outs. *Proceedings of the ACM on Human-Computer Interaction 4*, CSCW3 (2021), 1–27.

[85] RADER, E., WASH, R., AND BROOKS, B. Stories as informal lessons about security. In *Proceedings of the Eighth Symposium on Usable Privacy and Security (SOUPS)* (New York, NY, USA, 2012), Association for Computing Machinery.

[86] REDMILES, E. M., BODFORD, J., AND BLACKWELL, L. "I just want to feel safe": A diary study of safety perceptions on social media. In *Proceedings of the International AAAI Conference on Web and Social Media* (2019), vol. 13, pp. 405–416.

[87] REDMILES, E. M., KROSS, S., AND MAZUREK, M. L. How I learned to be secure: a census-representative survey of security advice sources and behavior. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (2016), pp. 666–677.

[88] REDMILES, E. M., MALONE, A. R., AND MAZUREK, M. L. I think they're trying to tell me something: Advice sources and selection for digital security. In *2016 IEEE Symposium on Security and Privacy (SP)* (2016), IEEE, pp. 272–288.

[89] REDMILES, E. M., WARFORD, N., JAYANTI, A., KONERU, A., KROSS, S., MORALES, M., STEVENS, R., AND MAZUREK, M. L. A comprehensive quality evaluation of security and privacy advice on the web. In *29th USENIX Security Symposium (USENIX Security 20)* (2020), pp. 89–108.

[90] REEDER, R. W., ION, I., AND CONSOLVO, S. 152 simple steps to stay safe online: Security advice for non-tech-savvy users. *IEEE Security & Privacy 15*, 5 (2017), 55–64.

[91] REICHEL, J., PECK, F., INABA, M., MOGES, B., CHAWLA, B. S., AND CHETTY, M. 'I have too much respect for my elders': Understanding South African Mobile Users' Perceptions of Privacy and Current Behaviors on Facebook and WhatsApp. In *29th USENIX Security Symposium (USENIX Security 20)* (2020), pp. 1949–1966.

[92] SCHEUERMAN, M. K., BRANHAM, S. M., AND HAMIDI, F. Safe spaces and safe places: Unpacking technology-mediated experiences of safety and harm with transgender people. *Proceedings of the ACM on Human-Computer Interaction 2*, CSCW (2018), 1–27.

[93] SCHEUERMAN, M. K., JIANG, J. A., FIESLER, C., AND BRUBAKER, J. R. A Framework of Severity for Harmful Content Online. *arXiv preprint arXiv:2108.04401* (2021).

[94] SIMKO, L., LERNER, A., IBTASAM, S., ROESNER, F., AND KOHNO, T. Computer security and privacy for refugees in the United States. In *2018 IEEE Symposium on Security and Privacy (SP)* (2018), IEEE, pp. 409–423.

[95] SLUPSKA, J., DAWSON DUCKWORTH, S. D., MA, L., AND NEFF, G. Participatory threat modelling: Exploring paths to reconfigure cybersecurity. In *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems* (2021), pp. 1–6.

[96] STASKO, E. C., AND GELLER, P. A. Reframing sexting as a positive relationship behavior. Drexel University, 2015. `https://www.apa.org/news/press/releases/2015/08/reframing-sexting.pdf`.

[97] SULLIVAN, N. *A critical introduction to queer theory*. NYU Press, 2003.

[98] TAYLOR, P. *A survey of LGBT Americans: Attitudes, experiences and values in changing times*. Pew Research Center, 2013.

[99] TAYLOR, S. H., HUTSON, J. A., AND ALICEA, T. R. *Social Consequences of Grindr Use: Extending the Internet-Enhanced Self-Disclosure Hypothesis*. Association for Computing Machinery, New York, NY, USA, 2017, p. 6645–6657.

[100] THOMAS, K., AKHAWE, D., BAILEY, M., BONEH, D., BURSZTEIN, E., CONSOLVO, S., DELL, N., DURUMERIC, Z., KELLEY, P. G., KUMAR, D., MCCOY, D., MEIKLEJOHN, S., RISTENPART, T., AND STRINGHINI, G. SoK: Hate, Harassment, and the Changing Landscape of Online Abuse. In *IEEE Symposium on Security and Privacy (SP)* (2021).

[101] TSENG, E., FREED, D., ENGEL, K., RISTENPART, T., AND DELL, N. A digital safety dilemma: Analysis of computer-mediated computer security interventions for intimate partner violence during covid-19. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (2021), pp. 1–17.

[102] TSENG, E., SABET, M., BELLINI, R., SODHI, H. K., RISTENPART, T., AND DELL, N. Care infrastructures for digital security and privacy in intimate partner violence. In *Extended Abstracts of the 2022 CHI Conference on Human Factors in Computing Systems* (2021).

[103] WADE, K., BRUBAKER, J. R., AND FIESLER, C. Protest privacy recommendations: An analysis of digital surveillance circumvention advice during black lives matter protests. In *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems* (2021), pp. 1–6.

[104] WALKER, A. M., AND DEVITO, M. A. "'More gay' fits in better": Intracommunity Power Dynamics and Harms in Online LGBTQ+ Spaces. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (2020), pp. 1–15.

[105] WALKER, A. M., YAO, Y., GEENG, C., HOYLE, R., AND WISNIEWSKI, P. Moving beyond 'one size fits all' research considerations for working with vulnerable populations. *Interactions 26*, 6 (2019), 34–39.

[106] WANG, Y. The third wave? inclusive privacy and security. In *Proceedings of the 2017 New Security Paradigms Workshop* (New York, NY, USA, 2017), NSPW 2017, Association for Computing Machinery, p. 122–130.

[107] WATSON, H., MOJU-IGBENE, E., KUMARI, A., AND DAS, S. "We hold each other accountable": Unpacking how social groups approach cybersecurity and privacy together. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (2020), pp. 1–12.

[108] ZENG, E., KOHNO, T., AND ROESNER, F. What Makes a "Bad" Ad? User Perceptions of Problematic Online Advertising. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (2021), pp. 1–24.

9 Appendix

9.1 Interview Protocol

9.1.1 Advice

1. Have you ever looked for or gotten advice related to online safety, security, or privacy concerns?
    - From where or from who did you learn to do this?
    - What were you specifically concerned about?
    - What was the advice?
    - Did you follow this advice?
    - If yes: How did you evaluate this method? E.g., how did you decide whether it would work for you? Did it work? Do you still do it? Have you changed this strategy over time?
    - If no: Why not? Have you adopted a different approach to this concern rather than what the advice suggested?
    - Do you have other approaches to this specific concern?
    - Any followup questions to establish threat model
2. If having trouble thinking of advice: Do you have any behaviors you've adopted because of online safety concerns?
    - Where did you learn to do this?
3. Other prompts: dating, sexting
    - Security, privacy
    - Related to queer identity, other identities
4. Have you ever provided advice related to online safety?
    - Who did you provide this to, and how did they receive this advice?
    - Where did you learn this advice from?
    - Other prompts: dating, sexting
    - Security, privacy
    - Related to queer identity, other identities
5. Have you ever had difficulties trying to find online safety information?
    - Have you had difficulties finding information that you felt connected with you and your life?
6. Are there behaviors you considered but didn't adopt?
    - Where did you learn about these behaviors?
    - What made you decide not to adopt it?
7. Have you ever used Google or another search engine to find online safety information?
8. Have you ever used social media sites themselves to find or ask for online safety information?
9. What online safety/security/privacy concerns do you have that you haven't found advice or haven't been addressed?
10. If there's free time: what do you think about x advice? From advice coding

9.1.2 General

1. Are there any particularly good or bad online safety advice sources you've come across?
    - What made it good/bad?
2. How do you define online safety? What does online safety mean to you?
    - Online privacy?
    - Online security?
3. What concerns do you prioritize the most?
4. Is there anything else you would like to share?

9.1.3 Demographics

You can say pass if you want to skip any of these questions.

1. Disability disclosure
2. Kind of area you live in: rural/urban/suburban?
    - How long have you lived there? Other places you've lived for a long time?

9.2 Advice Probes and Sources

9.2.1 Example Advice Probes

- Use Private Account
- Selective Sharing
- Block Users
- Disengage from Conversations
- Create New SM Reflecting True Gender
- Update SM to Reflect True Gender
- Delete, Untag Old Photos
- Don't Meet at Home
- Tell a Friend Where You are Going
- Use "Ask for Angela" Type Code Words
- Use Police Apps to Notify of Location
- Background Check Date
- Use Safe Dating Apps
- Only Download Apps from Trusted Sources
- Use Two-Factor Authentication (2FA)
- Use a VPN

9.2.2 Sources

- https://www.thetrevorproject.org/wp-content/uploads/2019/06/IG-x-Trevor-Project_LGBTQ-Safety-Guide.pdf
- https://www.vpnmentor.com/blog/lgbtq-guide-online-safety/
- https://www.comparitech.com/blog/vpn-privacy/lgbtq-cyberbullying/
- https://www.lgbttech.org/copy-of-online-safety
- https://www.hopkinsmedicine.org/health/wellness-and-prevention/tips-for-parents-of-lgbtq-youth
- https://www.thetrevorproject.org/2020/12/10/the-importance-of-safe-language-on-social-media/
- https://www.grindr.com/g4e/G4E-HolisticSecurityGuide-English.pdf
- https://forge-forward.org/resource/safe-dating-tips/
- https://staysafeonline.org/wp-content/uploads/2017/09/What-LGBT-Communities-Should-Know-About-Online-Safety.pdf
- https://www.centeronhalsted.org/transsafedatingtips0909.pdf
- https://queer-voices.com/online-dating-safety-tips-for-lgbtq/
- https://www.baltimorepolice.org/safeplace/safety-tips
- https://policies.tinder.com/safety/intl/en
- https://www.gayquation.com/safety.html
- https://nomadicboys.com/safety-gay-dating-apps/
- https://www.pride.com/lovesex/2019/3/24/3-easy-ways-stay-safe-while-using-dating-apps
- https://faze.ca/how-to-stay-safe-on-gay-dating-websites/
- https://avp.org/resources/safety-tips/
- http://www.galop.org.uk/wp-content/uploads/2016/11/Crime-Safety-and-Hook-Up-Apps.pdf
- https://www.loveisrespect.org/resources/dating-in-the-closet/
- https://www.thinkuknow.co.uk/professionals/our-views/how-to-support-lgbt-young-people-to-stay-safe-online/
- https://www.legalreader.com/online-dating-scams-how-to-stay-safe-with-online-dating/
- https://www.cosmopolitan.com/uk/love-sex/relationships/a19603997/online-dating-safety-tips/
- https://meanshappy.com/how-to-stay-safe-when-using-online-dating/
- https://socialcatfish.com/blog/lgbt-dating-apps/
- https://vpnoverview.com/privacy/apps/privacy-grindr/
- https://www.datingscout.com/tips/staying-safe-with-online-dating