Analyzing Usable Security, Privacy, and Safety Through Identity-Based Power Relations

Chris Geeng

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

Doctor of Philosophy

University of Washington

2022

Reading Committee:

Franziska Roesner, Chair

Tadayoshi Kohno

Elissa M. Redmiles

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

University of Washington

Abstract

Analyzing Usable Security, Privacy, and Safety Through Identity-Based Power Relations

Chris Geeng

Chair of the Supervisory Committee:
Franziska Roesner
Computer Science & Engineering

While privacy and security is an issue for everyone, lack of power in relation to adversaries leads certain individuals to experience different or riskier vulnerabilities. For example, as related to smart homes, children or non-technologically savvy occupants may not have the same degree of access to smart home functionality as the installer. Or as related to sexting, women are more likely to be blackmailed or threatened with their sexually suggestive or explicit content. To recommend technology design and policy changes to support privacy and security for marginalized communities, my research explores people's privacy and security concerns and behaviors in three different contexts: smart homes, sexting, and security advice. My latter two projects focus more on the LGBTQ population in particular. I use primarily qualitative and mixed methods to elicit rich, detailed anecdotes and data from participants, asking what threats do these users face, what makes it difficult for users to mitigate those threats, and what designs can remove or reduce threats? Through these methods, my thesis answers these questions for disempowered users in these contexts, including people marginalized across sexual orientation and gender, and shows how power relations to other individuals, culture, and societal institutions affect users' experiences and perceptions of security and privacy.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACKNOWLEDGMENTS

A great many people have been instrumental to my growth both as a researcher and as a person during my time in graduate school.

First, I am incredibly grateful to my advisor Franziska Roesner for the research knowledge she has passed onto me, her sense of perspective when I have struggled, and her kindness throughout these five years. She has always believed in my research ideas as I have zigged and zagged my way through my PhD, and her support has been invaluable to building my confidence as a researcher. The lessons I have learned from her will stick with me for the rest of my research career. And her commitment to advising students as a whole person, rather than just as a researcher, is my blueprint, and I hope to become as good of a mentor as her someday.

I thank the rest of my committee for their feedback and support: Tadayoshi Kohno, Elissa Redmiles, David Ribes, Jason C. Yip, and James Pierce. I am also grateful for my collaborators on my research in this dissertation: Mike Harris, Jevan Hutson, and Elissa Redmiles. I am especially grateful to Elissa Redmiles for her mentorship and expertise on security advice, and to David Ribes for teaching me about Science, Technology, and Society studies.

Thank you to everyone in the Security and Privacy Lab for the camaraderie, advice, and fun these five years: Christine Chen, Kaiming Cheng, Camille Cobb, Pardis Emami-Naeini, Ivan Evtimov, Earlence Fernandes, Umar Iqbal, Kiron Lebeck, Ada Lerner, Shrirang Mare, Peter Ney, Kentrell Owens, Lucy Simko, Anna K. Simpson, Miranda Wei, Tina Yeung, Eric Zeng, and everyone else who has passed through the lab. Thank you Tadayoshi Kohno and David Kohlbrenner for expertise on security history and wider-ranging research. Outside

of my lab, James Fogarty and Annie Ross were amazing for teaching me about organizing for DUB. Thank you to Ryan Calo, Audrey Desjardin, Alexis Hiniker, Catherine Holmes, Amy J. Ko, Jevin West, Ben Zisk, and the UW Statistical Consulting Services for their expertise. And PhD life would not have been the same without Elise deGoede Dorough and Joe Eckert's administrative support and morale-funded events. Thank you for all the help during this on-going pandemic.

I have had amazing mentors outside of University of Washington as well. I am thankful to Ignacio Contreras for my internship at Facebook's Safety and Integrity team, Alexandra To for guidance on ethics in academia, and Karen Levy for introducing me to the area of privacy and surveillance in the first place.

I could not have survived this journey without my friends! Thank you to my Dungeons and Dragons group for continuous adventures outside of school: William Agnew, Tal August, Tyler Baxter, Kimberly Dacorogna, Gabe Erion, Philip Garrison, and Sofia Serrano. I am especially grateful to William Agnew, Philip Garrison, Brian Hou, Kentrell Owens, and Naveena Karusala for social interactions during a tough 2020, and also conversations on how to do research better and to make academia better. Thank you to my amazing CSE 2017 cohort, and the other friends I have made along the way at University of Washington: Nicasia Beebe-Wang, Esther Jang, Matt Johnson, Amal Nanavati, Jasper O'Leary, Leah Perlmutter, Audrey Seo, Peter West, Erin Wilson, and so many others. I thank Emily Tseng for great discussions on the politics of security, and Sheamus Heikkila and Naviya Singla for helping me work through the concept of gender.

Thank you to the stewards and organizers for our union UAW4121. My life in Seattle has been livable and amazing through the wages and healthcare we have fought for.

Thank you to Andrea Haverkamp for supporting me through my last year in my PhD program. If the one thing I got out of moving to Seattle was getting to meet her, it would still all have been worth it. Eternal thanks to Jimmy Briggs, my research collaborator, confidante,

magic trick teacher, and most importantly, my friend. Thank you to my cat Pitou, whose addition to my thesis via walking over my Bluetooth keyboard was indispensable. And finally, my love and thanks to my mother and brother Mei-Hua Liu and Franklin Geeng, for supporting me while across the country, and making sure I would know how to adult while far, far, far away from family. I would be nowhere without you.

My work was made possible by the Reddit moderators of r/sex and r/gaysian, queer social groups, and the Seattle AARP for advertising my studies. And my work was supported in part by a UW CSE Fellowship, the National Science Foundation under Award CNS-1513584, and from a gift from Google.

DEDICATION

To all the queer and trans activists who have made my existence as a human and as a researcher possible.

Chapter 1
INTRODUCTION

Power is who is advantaged or disadvantaged within social interactions, and differential power relations can exist in interpersonal, community, cultural, and institutional relationships [35]. Power is fundamental to how society is organized, and determines anything from who cleans in the household, who gets paid more at work, or who can use the Internet without fear of being harassed.

Identity (e.g., gender, sexual orientation, race, or class) is one factor in determining whether an individual has more or less power in relation to other people or institutions. While the Internet, and other technologies like the personal computer and the mobile phone, were heralded as great democratizers, instruments to level the playing field of society, they have not solved issues of power disparities like sexism, homophobia, racism, and income inequality.

New digital tools can be used to harm others through these stigmas and organizations of power; for example, women still suffer from sexual harassment on anonymous online forums [42]. Being disempowered by society (oppression or marginalization) influences not only the adversaries people face when using technologies (e.g., homophobic harassers on social media), but also the severity of harm from that threat (e.g., queer youth in a homophobic home may not have access to emotional support after an incident). And people who are oppressed across multiple, intersectional axes of identity face worse outcomes [72, 120].

Given the connection of power to threat of harms, it is important in usable security to include power relations in the analysis of what security, privacy, and safety concerns

technology users have, and how do they address (or cannot address) these concerns. My research takes this approach in three different technological contexts: smart homes, intimate communication, and online safety advice. I detail these projects below.

1.1 Thesis Statements and Research Questions

Using primarily qualitative methods, I investigate how users' identities impact their power in relation to other users or adversaries in these three contexts, leading to different perceptions of security or privacy threats and mitigation strategies. Understanding user perceptions helps designers build more usable affordances for protecting users, or identify when there is no technological solution for a threat. I use qualitative methods because they are effective for understanding people's perceptions—their motivations, fears, and other emotions as colored by their past experiences.

My research questions for these projects, which focus on understanding user perceptions, are:

1. **Smart homes.** Smart home devices and platforms—including the Amazon Echo, Google Home, Samsung SmartThings, Philips Hue lights, Nest thermostats and cameras, and more—are increasingly ubiquitous in end-user homes. Unlike other popular personal technologies of recent decades, like laptops and smartphones, smart home devices, when placed in a shared environment, become shared devices that are used by and affect multiple people. However, today's smart home platform multi-user support is often controlled (by default or otherwise) by a single user who has the most power over other household members, giving rise to problems both practical and interpersonal. For example, a child may be unable to turn on their homes' smart lights when their parent is away. Given these challenges, my study asked:

    - What tensions and challenges arise between multiple users of a single shared smart home?

- How do existing smart device and platform designs exacerbate and mitigate these issues?
- How should smart device and platform designers best take into account these complex relationships and interactions?

To answer these questions, I used a mixed methods approach, combining qualitative interviews with experience sampling over a three week period with 18 people living in smart homes. These participants were largely "smart home drivers," i.e., those who make key decisions about device installation and use. I found tensions across a variety of stakeholders—including parents and children, roommates, partners, and non-occupants—and across several phases of smart device selection, installation, and use. By highlighting different relationships that coexist in one household and differences in power dynamics among users, e.g., landlords and tenants, my work highlights design issues that need to be prioritized to support the most vulnerable smart home users or bystanders. I continue my focus on vulnerable users in my next project:

2. **Intimate communication.** Sending or receiving nude or semi-nude photos and other media (often called "sexting"), made possible by the greater ease of sharing and accessing sexual media, is a common sexual behavior for adults in the United States [117]. Despite its capacity for positive effects (self-expression and intimacy building in consensual relationships [15]), it carries risks from cultural stigma. Threats related to sexting can range from a family member accidentally seeing sexts on the user's screen over their shoulder ("shoulder-surfing") to malicious ex-partners threatening to share non-consensual intimate imagery (NCII) on the Internet ("revenge porn"). Women and LGBTQ+ individuals, particularly people of color who are disempowered across multiple identities, are more likely to be targets of NCII [63, 138].

   Towards this end, my research questions were:

- What are users' general practices and experiences related to technology-mediated intimate communication?
- What are users' computer security concerns and threat models related to technology-mediated intimate communication?
- How do users mitigate or manage these concerns, using technical or non-technical methods?

I collected information from an anonymous mixed-methods survey of adults who have sexted at some point in their lives (N = 247), with the majority of respondents self-identifying as queer. Participants answered with whom, how often, and on what platform they sext, as well as their concerns and mitigation practices. One of our findings was that women disproportionately received unsolicited sexts and were disproportionately worried about that occurring, highlighting the necessity of understanding how sexism and other forms of marginalization affect intimate communication risks.

My intimate communication research provides examples of how marginalization, particularly across gender identity, increases certain security risks. I further explored how one's lack of power in society in relation to others due to one's identity affects one's safety concerns and potential mitigations they can take in my third and final project:

3. **Security advice.** Though security research has studied how a general population of users seek and adopt security advice [186, 188, 189], it has not specifically explored this issue with a queer population. However, LGBTQ+ (Lesbian, Gay, Bisexual, Transgender, Queer and/or Questioning) individuals face threats that straight and cisgender people do not, like interpersonal threats (e.g., being outed to family) and threats from outside their communities (e.g., homophobic harassment on social media) due to stigma around queer identities. Given the importance of researching queer-specific advice seeking, my research questions included:

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

To answer these research questions, I conducted qualitative semi-structured interviews with 14 queer individuals who differed across age, race, gender, sexuality, and socioeconomic status. To explicitly analyze power in this work, I used the framework of intersectionality, 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]. Queer individuals may also experience oppression along other axes (e.g., race), which can increase certain security risks or make it more difficult to mitigate them. Among our findings, we observed that (1) participants turned to their queer support groups for emotional support, in addition to advice, after experiencing a safety concern, and (2) multiple facets of identity affect people's perception and adoption of advice.

My general methodology is grounded in feminist standpoint theory, which posits that social knowledge and experiences are situated in a specific context, and that an individual's experience may not be the same as another individual's with a different identity. Therefore, my work centers on marginalized voices and situated (not universal) knowledge that may translate from one queer person to another in a similar context. I also acknowledge that my perspective and identity affect how I interpret my findings, so I disclose my position as a researcher who is queer and non-binary, and this perspective adds strength to my work.

1.2 Thesis Overview and Contributions

I now present an overview of each thesis chapter.

1. **Chapter 5.2: Background on Power Relations and Harms.** I first present prior research in critical theory conceptualizing power and marginalization of different communities. This then motivates my work on how lack of power can lead to differential harms in different technological contexts, which I expand on in the following chapters.

2. **Chapter 3: Smart Homes.** Results of my interviews and experience sampling of participants living in smart homes paint a picture of households where smart home use reflects existing relationship dynamics and power structures in homes (e.g., parent and child). And that use can cause some occupants to lose power over domestic tools; smart home drivers tend to have more access to functionality and data than passive users. I make recommendations for designers and researchers to help minimize these differences between co-occupants, to consider different relationship types, and to design for long-term use as children grow and people move in/out.

3. **Chapter 4: Intimate communication.** Via an online survey of 247 adults who sext, I find that adults navigate sexting using both technical strategies, such as disappearing messages, and nontechnical strategies, such as relying on trust. I show (similar to prior work) that men were less likely than women and non-binary individuals to be concerned about certain potential sexting risks and less likely to receive unsolicited sexts. Placing my results in the context of the sexual privacy framework, I suggest ways platforms can support autonomy, intimacy, and equality through platform affordances and policies.

4. **Chapter 5: Security Advice.** From interviews with 14 queer adults living in the United States, I found that participants did not generally adopt security advice. This was not only due to inconvenience or usability issues, but because the suggested behavior would interfere with their incomes or relationships with others. Participants often turned to their queer support groups for advice on other's experiences with the same safety concern; prior research mainly identified family, friends, and workplaces as advice sources. I recommend that advice adoption be improved by providing emotional

support, and that advice providers make more specific recommendations so people can determine if it will work for them, contradicting prior recommendations that advice be concise and one-size-fits-all. This work offers a case study for security researchers on how to use intersectional analysis with threat modeling, as well as a foundation for generating context-specific and population-specific advice.

Based on the cumulative observations of these three studies, *my thesis shows the role power and identity plays in different users' perceptions of security and privacy.* It thus provides an additional theoretical approach to usable security research that better investigates and supports marginalized communities.

Chapter 2

BACKGROUND ON POWER RELATIONS AND HARMS

Studying disempowered communities is not new to Security. Security researchers have understood the need to support marginalized populations and their specific security needs, like journalists [160], sex trafficking survivors [55], intimate partner abuse survivors [89], sex workers [27], refugees [207], etc., as well as support inclusive privacy [11].

But what makes a group marginalized? How does this occur? What does power relations have to do with it? These questions are important so we can understand why we as researchers focus on these groups, and identify what other communities or user groups may have specific security needs that researchers need to consider. In addition, answering these questions will help security researchers suggest recommendations to change the underlying conditions of marginalization (if relevant), in addition to supporting security for threats in the moment.

To answer these questions, I turn to scholarship in critical theory, a field focused on understanding oppression in order to eliminate it. In this section, I will discuss what critical theory encompasses and various associated theories, why I focus on intersectionality and the power analysis of the domains of power for my research, and then its relevance to my security research, building on the scholarship of Costanza-Chock in Design Justice [69].

2.1 Critical Theory and Marginalization

While there is no single "critical theory", as it covers different philosophy and social science approaches during different time periods [40], generally a critical social theory is "concerned in particular with issues of power and justice and the ways that the economy, matters of race, class, and gender, ideologies, discourses, education, religion, and other social institutions, and

cultural dynamics interact to construct a social system" [135], in order to "to create a world which satisfies the needs and powers of" human beings [125]. In short, critical theories seek to understand power imbalances and oppression, in order to create a democratic society where humans have the agency to make decisions about their own lives.

Kincheloe writes about power, "A consensus seems to be emerging among criticalists that power is a basic constituent of human existence that works to shape the oppressive and productive nature of the human tradition. Indeed, we are all empowered and we are all unempowered, in that we all possess abilities and we are all limited in the attempt to use out abilities." [135]. A marginalized group is disadvantaged in someway, and oftentimes this disadvantage is having less power in relation to the government or society at large. For example, journalists may be targeted by a fascist government who seek to control mass media; government institutions have more power than an individual or group of journalists. In another example, the LGBTQ community, in addition to being a population minority, may be legislated against to have restricted access to healthcare. I go more into detail of different contexts for power relations in Section 2.3.

Marginalization exists for different communities based on identity, and there are different critical theories associated with political movements to emancipate these communities from oppression. For example, there is feminist theory for emancipating women from the economic and cultural control of patriarchy, critical race theory for dismantling structural and interpersonal racism, disability studies for creating a society accessible to all, postcolonial theory to counter negative consequences of imperialism, etc. Most relevant for my work is Collin's intersectionality and its conception of power as relations across multiple domains [35], which I discuss below.

2.2 Intersectionality

Intersectionality, developed by Black feminists, is the concept that "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" [35]. Originating

from Crenshaw's working highlighting how Black women face specific discrimination from the government for being marginalized along two axes of identity: being both Black and female (versus being Black and male, or white and female) [71, 72]. The Combahee River Collective further wrote about needing to consider Black lesbians, who are marginalized across *multiple* axes of identity, when organizing for change [67]. As Costanza-Chock notes, for technology design to support multiply burdened groups of people, an intersectional understanding of race, gender, class, and other identities is necessary.

This framework is most relevant for my research on security advice for LGBTQ+ folks in the U.S. (Chapter 5) because this work also studies how other axes of identity, in addition to queerness, affects advice perception. And this framework is most relevant for my thesis because of a close-linked concept: domains of power.

2.3 Conceptualizing Power as Relations across Multiple Domains

An important component of Collin's work on intersectionality is domains of power: sites of power imbalances can occur across multiple domains (which often overlap) including: interpersonal relationships, relationships with community/culture, relationships with disciplinary structures, and relationships with institutions and structural organization [35, 120]. To understand marginalization, these power relations should be analyzed both via intersections of identity, as well as across these domains of power to see how "power, oppression, resistance, privilege, penalties, benefits, and harms are systematically distributed." [69]

One can use domains of power in threat modeling, as a user will face a greater risk of security or privacy violations when an adversary has more power in relation to them. For example, unrelated to marginalized identities:

- Interpersonal-based threat to a child: a parent posts public photos of their babies or children online, which a child may not be able to contest or understand the privacy ramifications.

- Cultural/communal-based threat to a messaging app user: the majority of a friend

group decide to use a non-end-to-end-encrypted messaging app, even if the user does not trust it.

- Disciplinary-based (rules-based) threat to an Facebook user: while a European Union citizen has the legally-protected ability to request access to and audit what data companies have on them because the General Data Protection Regulation would discipline companies otherwise, a U.S. citizen may not be guaranteed that data.

- Structural-based threat to a smartphone user: living in a rural area, someone might only have one option for a phone repair business, and if that business requires the user to give the phone passcode or remove it, the user is at risk of the repair technician snooping through their data.

One can see through these examples that 1) categories of domains of power are fluid and overlapping, 2) while power relations are not inherently bad, they can lead to risks of harm or decrease agency in addressing those risks, and 3) power imbalances with institutional structures require structural solutions for mitigating risk.

This method of analyzing power relations can also apply to marginalization. For example, LGBTQ individuals have less power than straight individuals moving through society because of the risk of homophobic and transphobic backlash in different contexts. And they have less power than larger cultural and structural forces. This cultural stigma can lead to threats around these domains of power:

- Interpersonal-based threat: a family member messaging an individual with homophobic content.

- Cultural/communal-based: a coordinated troll campaign sending transphobic messages to an individual on social media.

- Disciplinary-based threat: a social media company failing to moderate and remove homophobic posts because it is not a part of their Terms of Service or community guidelines.

- Structural-based threat: finding community on a social media site requires using public-facing hashtags, but these hashtags being public run the risk of being co-opted by a hate campaign.

These risks disempower LGBTQ individuals since they must navigate their lives avoiding these harms or dealing with the consequences from these harms. And these risks can be worse if an individual has another marginalized identity interlocking with being queer. Marginalization of LGBTQ identity adds another layer of disempowerment to individuals who may already face power imbalances in their relationships to their loved ones, communities, work, health, social media, and other institutions.

And as one can see through these examples, marginalization shows up as power imbalances between the marginalized and these domains. Throughout the rest of this thesis, I will sometimes use marginalization and imbalanced power relations somewhat interchangeably.

2.4 Power Relations and My Work

As I've shown in previous sections, differential power relations can occur in many forms, whether due to innocuous societal norms like family organization, or due to the societal marginalization of an identity group. And these power imbalances can lead to different security and privacy risks which are important to study in order to support disempowered individuals and communities. Drawing on the values of critical theorists, my goal for this thesis is to highlight power imbalances and imbalanced risk of threats in order to point out how structural changes are needed in addition to technological solutions to ensure equitable access.

For my first project on smart homes (Chapter 3), I focus on how interpersonal power dynamics in the home, such as parent and child or smart home installer and passive user,

affect privacy and access to smart home technology. My second project on intimate communications (Chapter 4) is motivated by how power imbalances between straight cisgender men and others lead to disproportionate impacts of sexual harms to women and non-binary individuals.

And finally, for my final project on security advice for queer individuals (Chapter 5), I use the framework of intersectionality, originating from Black feminist scholarship [120, 71] that theorizes oppression as interlocking axes rather than additive ones. I use this because this project is interested in how other axes of identity, along with queerness, affect people's perceptions of security advice.

In the following chapters, I discuss my research on power relations and harms with smart homes, intimate communications, and security advice for queer individuals.

Chapter 3

WHO'S IN CONTROL?: HOW POWER RELATIONS AFFECT INTERACTIONS IN MULTI-USER SMART HOMES

Households can be a site of uneven power relations, e.g., parents and children, landlords and renters, and controlling partners, which determine what people can do or change in a house, and how in control people are of their privacy.

Smart home devices—Internet or local-connected devices that can automate or allow remote control of domestic utilities—add another layer of complications around in-home agency, as domestic utilities can be controlled or surveilled remotely through the Internet, and may have limited multi-user support. To explore how differential smart device control might arise in smart homes, this chapter looks at conflicts and privacy concerns in multi-user smart homes.

The material in this chapter first appeared as: Who's In Control?: Interactions In Multi-User Smart Homes. Christine "Chris" Geeng, Franzi Roesner. ACM Conference on Human Factors in Computing Systems (CHI), May 2019 [98].

3.1 Motivation and Overview

Smart home devices and platforms—including the Amazon Echo, Google Home, Samsung SmartThings, Philips Hue lights, Nest thermostats and cameras, and more—are becoming increasingly ubiquitous in the homes of end users. Unlike the popular personal technologies of recent decades, like laptops and smartphones, smart home devices, when placed in a shared environment, become *shared* devices used by and affecting multiple people.

However, today's commercial smart home platforms often provide only limited multi-

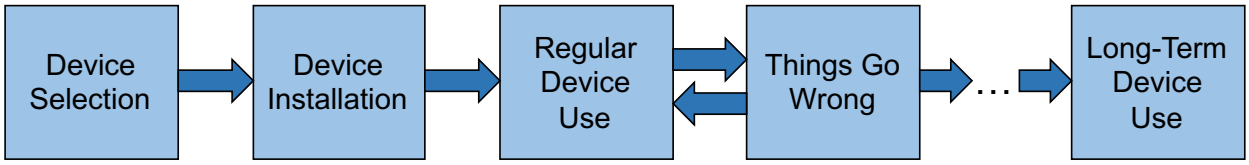

Figure 3.1: Smart Home Usage Timeline: Our study reveals multi-user tensions and interactions at several points during device installation and use.

user support. For instance, in the case of SmartThings, end users can provision multiple accounts but cannot currently give them different levels of access to information [14]. Prior research has surfaced the need to study multi-user issues in smart homes in more depth (e.g., [240, 162]); taking advantage of the fact that smart homes are now deployed beyond early adopters, we study multi-user device sharing *in situ* among a variety of households.

In this work, we systematically study the interactions between multiple people in contemporary, deployed smart homes, asking: What tensions and challenges arise between multiple people? How do existing smart device and platform designs exacerbate and mitigate these issues? And how should smart device and platform designers best take into account these complex relationships and interactions? we investigate these questions using a mixed methods approach, combining qualitative interviews with experience sampling over a three week period with people living in smart homes. These participants were largely "smart home drivers", who make key decisions about device installation and use.

Our findings (Section 3.4) reveal tensions that arise among a variety of stakeholders—including parents and children, roommates, partners, and non-occupants—and across several phases of smart device selection, installation, and use. For example, we often observe a concentration of expertise, access, and control with the person who selects and installs smart devices in a home, which extends and reinforces prior work (e.g., [162, 240]). At the same time, we were surprised to find limited reports of concern about privacy between people in the home. This limited concern may be due to selection bias: our participants, mostly smart home drivers, may have been unaware of other or more serious concerns held by more passive

users.

Our interviews also surfaced challenges that arise during the long-term use of smart devices: for example, what happens—or what should happen—when children grow up or house occupants change? From these and other findings, we distill lessons and recommendations for smart home designers, as well as identify opportunities for future research.

3.2 Background and Related Work

I use the term "smart home" to refer to a home that contains computing devices that assist with automation, remote usage, and/or sensing for domestic use. This term can and often does overlap with the Internet of Things (IoT), which broadly refers to Internet-connected devices (though some smart home devices can function on a local network).

A variety of smart home technologies are becoming commercially available and are on the cusp of widespread deployment [196]. Common smart devices in today's homes include thermostats (e.g., Nest [170]), light bulbs (e.g, Philips Hue [127]), outlets, door locks, motion sensors, TV streaming devices, smart assistants, and indoor/outdoor security cameras. Smart assistants such as Google Home [99] and Amazon Echo [20] include functionalities such as music playing, web search, reminders and timers, and voice command controls for devices connected to it, such as lights. Also commercially available are smart home hubs, such as Samsung SmartThings [211], which provide centralized control for devices that may come from different manufacturers.

3.2.1 Living in Smart Homes

Early "in the wild" user studies with smart home devices focused on understanding technical barriers to adoption (e.g., [45]). With improvements to smart home technology, user studies have moved towards exploring and evaluating how device designs do or could fit into domestic routines and home life, e.g., [162, 164, 163, 128, 237, 236, 131, 238], as well as other shared physical environments [212].

A particular recurring issue in prior work, reinforced and expanded by our study, is the

different levels of access and ability among different people in the home [51]. For example, Bell et al. (2007) called for the study of how ubiquitous computing could reproduce existing power concentrations in relationships [29]. Specific to smart homes, both Mennicken et al. (2012) [162] and Zeng et al. (2017) [240] recognized the need to support household members who did not initiate smart home installation and do not have the same expertise and agency as installers. Our work aims to explore and study these and other tensions that arise in multi-user smart homes *in situ* and in more depth.

3.2.2 Privacy in the Home

User privacy, defined as maintaining "control over personal information" [213], is often a concern in the design of ubiquitous computing environments more generally [30, 124, 178, 126], as well for smart homes in particular.

Prior work has explored in-home privacy from third parties such as device manufacturers, advertisers, and the government [241, 25, 52, 240], as well as the effects of home surveillance by researchers [176]. Choe et al. (2011) surveyed what moments in a home that people would not want recorded [60], but did not make explicit who might have access to recordings. In our work, we explicitly study interpersonal privacy between household members in a smart home, rather than from external parties.

Personal data monitoring within households raised concerns even before contemporary smart home devices [59]. Choe et al. (2012) studied when and why people would want motion, electrical, and video sensing in the home, and surfaced tensions between couples, between parents and children, and between households and visitors [61]; they found that couples were concerned about recordings in case of divorce, and that parents had internal conflicts over telling their children about recording and wanting to be able to watch them. This study used functionless probes and dates to when smart home devices were not yet mainstream; our work updates our understanding of contemporary smart devices deployed organically (i.e., not for research purposes).

Privacy concerns beget access control questions: how should data and device access be

controlled among household members? Earlier work on personal data sharing and access control in homes studied digital devices meant not for controlling physical space, but for file storage (such as computers, mobile phones, and music players) [153, 154], whereas more recent work has considered access control for users of smart home devices (e.g. [225]). He et al. (2018) found that multi-user smart home consumers would prefer control at function-level granularity rather than per-device access control [116]. Smart home devices differ significantly from earlier digital devices shared among household members: they sense and control physical space but often lack screens, making it difficult to rely on traditional interactions for indicating privacy [132] or to use visualizations for supporting awareness [131].

The tension of parents wanting to monitor their children while also respecting their privacy appears in parenting technology research more generally (e.g., [73, 226]); prior work has also studied the privacy and other concerns around home technologies for older adults (e.g., [76, 222]). Smart home devices in shared physical spaces will further press on these issues for both populations. Finally, Hoyle et al. (2014) also considered privacy for incidental users who pass through a device's physical space, rather than device owners, in the context of life-logging cameras [126]; similar issues may arise for people in smart homes.

3.3 Methods

Our study consisted of three components. First, we conducted a semi-structured interview that lasted between 15 and 60 minutes (varying based on how many devices the participant owned); second, if participants chose to continue the study, we collected three weeks of experience sampling data; third, we conducted a semi-structured exit interview. Interviews were conducted in-person on our university campus or by video call. The study protocol was approved by our institution's human subjects review board (IRB).

3.3.1 Procedures

During the initial semi-structured interview, we asked questions about which smart devices our participants had, how they used them, who installed the devices, and whether any

tensions had arisen between them and other people who lived or came into the home. We also asked if participants had ever learned anything surprising about their co-occupants through the smart devices or vice versa. To avoid priming participants, we avoided using the word "privacy" explicitly unless a participant brought it up first.

We then collected three weeks of experience sampling data via a smartphone application that we developed for Android and iOS based on an open source template [220]. We asked participants to use the app to log any experiences that they considered a "tension" in their house with another person related to a smart device. These incident logs were submitted to the research team. The app reminded participants about the study every three days. We used experience sampling, rather than asking participants only to recall past incidents during the interviews, in the hopes that participants would provide more logs and more accurate details logging the events as they occurred [68].

At the end of the three-week experience sampling period, we conducted an exit interview with participants to ask follow-up questions about incidents that were logged. Participants were initially paid $20 for the initial interview, $7 per week of logging (regardless of the number of logs submitted), and $20 for the exit interview. After calibrating during the first several participants based on how much time the interviews and logging activities actually took, we adjusted compensation to $20, $3 per week, and $10 respectively for each study component, in consultation with our IRB.

3.3.2 Recruitment

We recruited subjects by sending recruitment flyers electronically through online communities interested in smart homes, through personal networks on social media, and through local high schools. We also posted physical flyers around a university. Interested participants were directed to fill out an online survey, which we used to collect information about which smart home devices they use or want to use, as well as their comfort level with technology.

3.3.3 Participants

Table 3.1 summarizes our 18 participants (4 female, 14 male), who range in age from 17-44 and all live in a home with smart devices and share the home with at least one other person. P15 lives in Australia; everyone else lives in the United States from various states. All participants come from different households. All 18 participants completed the initial interview, 14 participants completed the experience sampling section (Table 3.1 lists how many logs each person submitted), and 11 participants completed all three sections. In our results, we will use the term "smart home driver" to refer to participants who instigate using smart home technology (primarily through installation) and the term "passive user" to refer to people less involved in smart home decision making. These terms are adapted from the smart home roles introduced in previous studies; they are not meant as value judgments, but as a categorical convenience [184, 162].

Our participants represent a variety of co-habiting situations (with a partner or spouse, with roommates, with children, with parents). Specifically, three participants were college students who lived with roommates; 14 participants lived with their partner and/or other family members; one participant is an adolescent. We aimed for variety in household relationships, but found it difficult to recruit a larger number of households with adolescents or roommates. We also found it difficult to recruit more passive users (perhaps in part due to recruiting from smart home enthusiast forums). We were unsuccessful at recruiting other (passive) household members of our smart home driver participants.

3.3.4 Data Analysis

From the 14 participants who completed the three weeks of experience sampling, we received 46 logs, at an average of 3.3 logs per person. The number of logs per person ranged from 0 to 9. Most logs pertained to issues that arose involving a device and more than one person, and we used these entries as discussion points during exit interviews. Some logs described technical issues that only affected the logger. People who owned more smart devices tended

	Gender	Age	House Members	# of Logs	Smart Home Role	# Device Types
P1	Male	26	Girlfriend	3	Driver	19
P2	Male	37	Mother	2	Driver	3
P3	Female	24	Boyfriend	0	Driver	1
P4	Male	34	Girlfriend	9	Driver	15
P5	Male	23	3 Roommates	3	Passive User	3
P6	Male	38	Wife, daughter, son	9	Driver	13
P7	Female	38	Husband, 2 daughters	1	Driver	11
P8	Male	29	Wife, daughter	N/A	Driver	6
P9	Male	33	Wife, daughter	3	Driver	10
P10	Male	17	Mother, father, sister	N/A	Driver	1
P11	Female	24	2 Roommates	N/A	Driver	2
P12	Male	43	Wife, son, daughter	3	Driver	6
P13	Female	20	7 Roommates	1	Passive User	1
P14	Male	30	Wife	1	Driver	6
P15	Male	44	Girlfriend stays over part-time	4	Driver	6
P16	Male	34	Wife, 2 children	3	Driver	6
P17	Male	37	Wife, daughter	4	Driver	6
P18	Male	29	Wife	N/A	Driver	8

Table 3.1: Study Participants. We detail participant demographics, how many experience logs they submitted during our study, their role in the smart home, how many types of devices they reported having. "Type" here refers to the kind and brand of device, not an individual unit (e.g., owning two same-brand smart bulbs is classified as "one type").

to submit more logs.

We transcribed the audio recordings of the interviews, and we took an inductive approach to coding the transcripts and logs. Two researchers read several interviews, developed codes, compared them, and then iterated again with more interviews until we had developed a consistent codebook. The final codebook consisted of 35 codes in total. Then each researcher coded half of the interviews, frequently checking in with each other whether any codes needed to be added or changed. After all interviews had been coded, both researchers spot-checked the others' coded transcripts and did not note any inconsistencies. Finally, we further organized and taxonomized our codes into higher-level categories.

3.4 Results

From our interview and experience sampling data, we identified several chronological points during smart home implementation and usage when significant multi-user interactions or tensions arose (Figure 3.1): (1) device selection and installation, (2) regular device usage, (3) when things go wrong, and (4) over the long-term, as changes occur in the home. We organize our results according to this timeline.

3.4.1 Device Selection and Installation

We begin by considering how participants and their co-occupants select and install new smart devices in their homes. 15 of the 18 participants had personally installed at least one device in the home. 14 of these participants were the *only* occupants in the home who had installed these devices.

Device Installation Decisions

Some smart home driver participants explicitly consulted with their co-occupants over which smart devices to get: P8, P18 and P7 all consulted with their partners, reporting that their partners were also interested in the devices. P7 qualified this, reporting that the main reason to consult each other was if the device was expensive.

Other participants selected devices independently but anticipated co-occupant's concerns. For example, P16 lives with his wife and children, and he is aware of his wife's concerns. Initially, "I didn't really ask, I started installing them, but then my wife [said] some of them are kind of ugly and unsightly so you have to find different ways to place them." After learning about her preferences for aesthetics as well as functionality, he was better able to decide what to purchase.

Finally, many participants explicitly did not consult with co-occupants about the decision to install smart devices. Participants who did not consult their co-occupants often discussed the other person's disinterest or passivity with respect to smart devices. For example, P1, P6, P9, P14, and P17 all said they were interested in devices while their partners were not. P1, when asked about whether he would be the only person making changes or additions to the smart home, said, *"[My partner is] a passive person, she doesn't care that much about it, it's definitely me all the way."*

Sometimes the passivity of co-occupants changed after the first devices were installed. For example, when P6 was asked if there were disagreements with his partner upon installation he said, "No. She...wasn't too interested. Now that she's seen usefulness, she likes it better." P9's partner had a different experience: *"[My wife] was sort of indifferent to [the smart home] when it first started, and then I started expanding it...I think she doesn't necessarily like having all these gadgets...[but] I don't think it's that big of a deal to her."* P9's wife does not whole-heartedly like the smart home.

In other cases, smart home drivers did not consult co-occupants because they did not consider them equal decision-makers in the home. P2, whose mother lives with him, said he did not consult her because it is his house, and if he shared the house with an equal partner, he would consult them first (though his mother eventually grew accustomed to the smart devices). P15's partner spends several nights a week at his place but does not live there, and P15 did not consult her about installing Hue lights with a timer and motion sensors.

Account Management

The process of installing smart home devices or platforms often involves creating new accounts, or linking devices to existing accounts. Several participants created separate accounts for people in their home because the service in question made it easy to do. P9, who owns a Google Home and Nest products, set up separate accounts for himself, his wife, and his daughter, as they are all using Google accounts. Once the separate accounts were set up, P9 appreciated the privacy it provided: "I like to just have the stuff separate. So, [my wife] can sign out of it and have sort of her own privacy with it."

In other cases, service providers did not make it easy to create multiple accounts. P12 mentioned that Ecobee (thermostat) did not have an option to allow his wife to set up her own account. By contrast, he was able to do so with Ring (doorbell): "It was a lot easier for her to set up an account [with Ring], so I prefer to do it that way."

Frequently, the use of a single account reflected the disproportionate control or interest of the device's installer. For example, P17's wife uses his account for their Apple Home, and his wife "thinks it's cool and all that, but she's not as motivated to do it." For P5, P11, and P13 who live with roommates, the account for the device was solely the account of the person who bought the device. For most other participants, they had installed the device and so they had their co-occupants share their account.

Some participants shared accounts for other reasons. For instance, P3 described a relationship dynamic in which many things are shared: "My boyfriend and I have each other on Google Maps so we track each other anyway. You can do location sharing permanently. We share everything, [including an] Amazon Prime account. So it makes sense to share the Alexa. Our fingerprints open up each other phones. We're pretty transparent."

3.4.2 Regular Device Usage

After devices are selected and installed, they are integrated into home life. Our data revealed a number of multi-user issues that arise during ordinary use of installed devices.

Agency of Installer

First, we observed the smart home driver having outsized control over smart device data and functionality, as compared to other home occupants. This situation often arose by *default*, as an extension of the installer's agency around device selection and installation in the first place (described above). Other occupants sometimes have less interest in the devices, limited technical ability to control them, or both. For example, P4 says about his girlfriend, who moved in after he started setting up his smart home: "[She says] 'I don't know what I'm doing [with smart devices],' and I try to teach her, but I don't think she wants to know."

When only the device installer has access to the device's account, functionality is limited to this user by default. For example, P10, who lives with his parents and sister, owns a Microsoft Invoke, which is connected to his Microsoft account. Only he has access to the history of voice command searches made with the device.

In other instances, the device installer *purposely* limited access to certain functions. For example, P6 added his 8-year old daughter as a secondary user in the Apple Home app, which centralized control of smart devices. By adding her as a secondary user, P6 prevented her from taking administrative actions like deleting a device.

Information Sharing and Privacy

Unlike traditional homes, smart homes collect significant amounts of data about their occupants, including voice recordings, browsing history, door opening, and other usage data [119, 70, 215], as well as access to potentially sensitive data such as emails [70]. This data is often surfaced to the users of the smart devices; for example, devices like the Amazon Echo allow users to see a history of commands and replay the voice recordings. Going into our study, we asked: Are people who regularly use these devices aware that this data is collected and accessible to co-occupants? Are they concerned or bothered by this?

We found that several installers, including P9, P12, and P16, were aware of the information that their smart devices collected from the whole house. P9 was neither surprised nor

particularly concerned: "I can track everything that the Google Home hears through their app...The only thing I do [think] that is a little weird is that the Google Home will, every now and then, just turn on 'cause I think it thinks that somebody's saying the hot word....but it doesn't really tell anybody any of my information that I'm worried about getting out."

P12 was also not surprised, but his wife "was surprised at how much...[Google Home] actually kept. And that you could go back and see...what you requested..." Despite this, his wife was not concerned: "You know, now she's just aware that...because she's the parent she has access to the kids' [record, which she likes], but unless you know she has access to another person's account, you know she won't be able to see it. It's private between you and Google." His wife trusts him and, by transitivity of his trust, trusts Google with the information collected by the device, and appreciates the access it provides to her children's information. P17 also liked the increase in available information afforded by the installed devices. He said, "The weird thing now is we know whenever somebody comes or leaves, because you get a door open notification... I sort of like it. [My partner] hasn't commented on it, but usually it's just the two of us, so it's just nice to know the other person is home."

By contrast, P5 was surprised when his roommate, who owns the Google Home, replayed the history of voice commands to all of their roommates. Afterwards P5 stated that "we got to know that [device owner] records our voices." In this instance, P5 was also ultimately not concerned: "It's super hilarious. We wanted to hear our voices being played."

One exception to lack of concern came from P6, who anticipated the concerns of another family member, his now 8-year-old daughter. When asked when he removed the internet-connected baby camera, P6 said they "stopped using it by default.... when she was two. But not because, we would have used it longer, but because of [moving to a different city and moving it to our son's room]. She deserves some privacy too. So we probably would have stopped maybe around [age] 5ish?" His child's personal privacy was a concern for him, although it was not the explicit reason why he removed the camera in this case.

Instead of concerns about interpersonal privacy, we heard more concerns about privacy with respect to the companies collecting the data. P14 and P15 both run their smart devices

on a local server so that their data doesn't go to a third-party server owned by the device company. P16 stated, "I think for a while we turned Alexa off, because it was just listening all the time and so if we're not getting enough value from home automation, we'll probably turn her off."

Preferences for Analog Devices

Even after smart home integration, we found that people often used or set up analog controls of devices as a backup. For example, P4 mentioned that his girlfriend "likes light switches. The way [the smart home is] set up, you have to leave the light switches off. So I taped over the light switches. Infuriated her." P4 stated that his girlfriend adjusted to it after about a year, after she learned she could control the fan as well as the lights using voice commands.

P9 and P15 both installed analog controls as an alternate control system in addition to motion sensor lights and voice command lights. P9 states, "My wife's a little old school, which is why I installed the light switches and not the bulbs, because she's still very manual, and so she just likes to turn the lights on and off." Analog controls worked except in the case of P6's 3 year old son: he is too short to reach the lights switches, but he also doesn't know the correct wake word to get the Amazon Echo to change the lights.

Playful Behavior

Our data contains a number of cases where smart device use was a source for fun, joking, or accidental laughs among co-occupants. For example, P2 logged that he "laughed when my mom gave her command before I did," when they were both trying to get his Amazon Echo to do something. The two of them have had several light-hearted standoffs attempting to gain control of the Echo, which were resolved by whoever stayed in the room the longest ultimately gaining control. In addition, one of P5's roommates has a Philips Hue Light Strip installed in his room, which is connected to the Google Home. P5 reported that he and his other roommates would sometimes turn off that roommate's lights for fun. In response, "he either comes down, or doesn't care." As a final example, P12's 10-year old daughter will, if

he's not at home, "ring the [smart] doorbell and try to get me to answer it [remotely on my phone]."

A few additional instances were still lighthearted but began to hint at sources of possible conflict. When P14 had guests over, they tried to use Amazon Echo voice commands to place orders from Amazon. P14 was annoyed about that, but had the ordering functionality disabled. And when P15's installation of proximity-sensing lights didn't work for his girlfriend's phone, he said she reacted, "'Haha told you it wouldn't work.' It's a little bit annoying but nothing serious." Trust likely plays a factor in the ability of people sharing devices to playfully interact; in this case his girlfriend trusts him to get the device to work eventually.

Though these instances of playful behavior were just that—playful—they suggest potential ways in which co-occupants can come into conflict over smart devices.

3.4.3 When Things Go Wrong

We now turn to what happens when "things go wrong"—when conflicts or tensions arise between people in a smart home, or how people interact when devices do not work as expected or intended.

Tensions and Conflicts Between People

We begin by considering conflicts and tensions that occur when devices work correctly (i.e., as intended by the manufacturer, designer, and/or device installer) but come up against mismatches in expectations or desires between different people in the home.

Partners An example of tension between partners occurred when P4 and his girlfriend had disagreements about their cleaning lady's access to the house. P4 stated, "I didn't want to give out our [door lock] code... One of the times she gave the cleaning person her code. I said I really don't like that because I've kind of set up these codes so that we have access to it, but we can take it away. This is like having a key, the way you get your key back is just

delete the code. We had a discussion about in the future don't give out the code... 'Cause this is my whole grand idea of the smart house." Part of the source of this tension may have been the fact that P4 is also the only one in the house with the knowledge for adjusting the smart devices, so his girlfriend may not have been able to create a new access code without his help.

P1 is also the sole smart home driver in his home with device knowledge, leading to tension with his partner who cannot change device controls. P1 logged that his girlfriend was annoyed she could not use the voice command "turn off TV" to turn off the TV, since P1 has Apple, Chromecast, and Fire TV, each requiring a specific command, e.g., "turn off Fire TV". In response, P1 set the general command to default to controlling Chromecast.

Roommates We also observed tensions between roommates, who have a different type of relationship. Between roommates, there is often one person to whom the device belongs, and there is less of an assumption of shared access and control rights as there may be between partners.

For example, P11, a college student, has a Nest Thermostat installed by her landlord in her apartment, where she lives with another student and a young professional. P11 took over use of the thermostat from the previous tenants and is the only one in the house who has the Nest app on her phone. P11 prefers a warmer temperature, while her roommate does not like when the air gets too dry. P11 says, "So sometimes [my roommate] will turn off the thermostat before she goes to bed and then I will pull up [the Nest app on] my phone [and] turn it back on. She knows that though." As to why her roommate does not also get the Nest app, P11 posits that the thermostat is physically close to her roommate's room and she can just change it manually. "We're not like super strict about how the temperature should be, so we never fight or feel uncomfortable with this temperature thing."

P13 is another college student who lives with roommates. One of her roommates owns an Amazon Dot, which the roommates use to play music, ask questions, and other functions. While P13 would say that everyone has equal access to the Dot, "we also know that this

device belongs to one person, so if for some reason she's using it, obviously she has priority over everyone else [using it] because she's the one that paid for it." These roommates resolve conflicts by deferring to the default control and agency of the device's installer or owner, a recurring theme in our findings.

P10, a teenager living with his parents and 13-year old sister, has also experienced tension: his sister sometimes uses physical control of a smart device as leverage in a conflict. For example, P10 reports: "I was like five minutes late to pick her up from school or something, and she gets a little bit mad about that. Then, she'll try to take away the smart device so it's hers." However, she cannot use it because P10 will remotely lock the device, since it is connected to his account. "She gives it back, of course." In this case, control of the device requires more than just physical control.

Parents and Children As conflicts naturally arise in parent-child relationships, conflicts also arise around the use of smart devices in the home. For example, we heard about parents and children competing for control over the Amazon Echo. In addition to the playful competition between P2 and his mother (discussed above), P16 has also vied with his 5-year old and 3-year old child for control of the music selection via the Echo at the dinner table. "Their favorite songs now are like the Pokemon theme song and 'What Did The Fox Say?'...so they'll just yell at Alexa and be like, turn it up to volume ten and let's go for it.... sometimes we would turn it back... I guess if we got really frustrated we would actually mute Alexa, so she wouldn't take any more commands during dinner."

Some parents explicitly used smart devices as parenting tools for setting limits or managing schedules, a recurring theme in smart home literature [237]. P10's father uses the Microsoft Invoke to add chores to P10's calendar, which the Invoke will verbally remind him to do. "He just sets reminders for us, which is kind of annoying, but what are you going to do?" Also, P9 installed an LED smart light and a Google Home Mini in his 4-year old daughter's room because she didn't like her room too dark, and P9 automated it to gradually turn off to signal to his daughter when it is time for bed. However, this scared her because,

"she feels she has no control over how it behaves... She doesn't like it in her room. She won't talk to it ever." This incident led his daughter to be uncomfortable with smart devices, as she is afraid of their behavior she cannot predict; she refused to keep a Google Mini in her room because of its blinking lights.

Guests and Non-Occupants Participants reported a number of cases in which guests or other people entered their homes and interacted with the smart devices, sometimes leading to conflicts or tensions. For example, P5's roommate owns the house's Google Home. This roommate was annoyed when P5's sister stayed over and used the Spotify account he had connected to his Google Home to play music that he did not like, since it changed future Spotify recommendations for him. In this case, guests having equal access to functionality led to consequences for the device owner.

When Devices Malfunction

Conflicts or tensions also arose when devices malfunctioned, either through a technical failure or by not working as the installer intended (e.g., because a smart home automation was improperly programmed). For example, a timer for a heater wouldn't go off, or a smart lock wouldn't register that someone's phone was in the vicinity. In this section, we consider how co-occupants interact in these cases.

First, we often observed that other home occupants were reliant on the smart home driver to fix the issue (in the meantime manually controlling the device by analog means, if possible). For example, P15 tried to set his heater to turn on automatically when he or his girlfriend were at his home. When it did not work, it fell on P15 to fix the issue, while they used manual controls in the meantime. Since smart devices may represent critical home infrastructure—including lights, temperature, locks, heaters, and other appliances that use electricity—relying on the smart home driver to fix these devices when there are no backup analog controls may put other home occupants in adverse situations. This is particularly the case with DIY smart homes, which may be less reliable than traditional homes where the

critical infrastructure is set up and wired by external experts (e.g., electricians).

We also heard frequent complaints about smart device voice commands not working as intended, particularly for less experienced or savvy users. For example, P6's 8-year old daughter "asked Alexa to turn on 'bedroom' light. Being that there are multiple 'bedrooms' set up in my home automation system, if there is a general request as in 'turn on bedroom light', Alexa should ask for clarification as to what bedroom the user is referring to." P6's suggestion hints at a way that smart devices could be redesigned to help guide less experienced people to use them more independently without relying on intervention from the smart home driver.

In other cases, even the smart home driver could not fix a fundamental issue. For example, P6's smart light setup relies on the smart home knowing someone is home. Because P6's children didn't have their own phone at the time, the house failed to recognize they were around: "My wife and I were out...[our phones] outside the geofence, but my kids and the babysitter were still at home. So [the lights] thought we were away... And for whatever reason, the motion didn't pick up that they were there." Asked when he would get his children their own smart phones, P6 said: "Probably around maybe 14 to 15, somewhere around there." Until then, the smart home may not be fully functional for P6's children, putting the intended functionality of the smart home at odds with P6's parenting choices around smart phone ownership.

3.4.4 Long-Term Use: Changes in the Home

Finally, our results surface how relationships between people and with smart devices may change over time.

Children Grow Up

Several participants mentioned changing their smart device interactions as their children grow older. For example, P6 has a Ring doorbell which sends a notification to his and to his wife's phone when someone is at the door. When his children are older, he plans to buy an

additional smart door lock so he can give his child a unique access code which will open the door and also notify P6 who opened the door. Recall also P6, discussed above, who noted that while his daughter's baby monitor camera was removed when they moved, he would have still removed it "maybe around [age] 5ish" because "she deserves some privacy too."

Occupants Change

Occupants of a home may change over time, though the smart devices installed in that physical space may stay behind. What does this mean for the configurations of these devices, as well as the potentially private data they store and make accessible? For example, when P11 moved into her apartment, she noticed that the landlord had installed a Nest Thermostat, and the previous tenant had not deleted their old account from the device; P11 deleted the account to connect the Thermostat to her own account.

In another case, a participant discussed theoretically what he would do if he moved out of his home in the future: he planned to leave his smart devices behind, viewing them as intentionally integrated with the specific physical space rather than personal devices he would take with him: "[all these devices] I'd think I'd leave, 'cause hopefully they'd be useful to other people."

3.5 Discussion

We now step back to consider the broader issues raised by our findings for multi-user smart homes, and we make recommendations for smart home designs and future research.

3.5.1 Differing Agency For Smart Device Access

A major theme throughout our results are the differences in power, agency, technical skill, and technical interest among different people living in a smart home. There is often a smart home driver who takes initiative to learn about and use devices, and passive users who adapt to devices and/or rely on smart home drivers to make changes. Practically speaking,

this means smart home drivers often have access to vastly more functionality (including the ability to set permissions for functions co-occupants can use) and more information (such as knowing when someone opens and closes a smart-locked door) than passive users. Our findings reinforce and expand upon those from prior work [240, 45, 162], and we observe that this dynamic is becoming increasingly concerning for technology-enabled abuse [41] as commonly deployed smart home devices expand from thermostats and lights to more security- and privacy-sensitive devices like digital assistants, smart locks, and smart door bells.

In some cases, this power difference simply reflects existing power dynamics in co-occupant relationships (such as parent and child). In other cases, the inclusion of technology can exacerbate these dynamics or allow for increased control or abuse by the smart home driver. For example, smart homes allow remote access to important household resources such as lights, heating, and door locks, breaking the assumption in a "dumb" home that physical access to a device allows—and is necessary—for controlling it. Likewise, managing a smart home requires some technical ability, which may widen the gap between people in the home when something goes wrong (e.g., a device malfunctions or the network goes down).

Limited Concern in Our Sample

In our study, we found that none of our participants expressed particular concern over these power differences, nor about issues related to interpersonal privacy. We see several possible reasons for this lack of concern. First, we interviewed people who reported being in stable, generally trusting relationships; other work has highlighted the importance of considering the role of smart home technology in cases of domestic abuse and intimate partner violence [152, 41, 54]. Second, our participants may have incorrect or incomplete mental models about the data collected by or accessible via smart devices and what private information is implied by this data [240, 123]. Finally, most of our participants are smart home drivers; other passive users may have different thoughts on this dynamic.

Gender Differences

We observe that the majority of smart home drivers that we interviewed were men. These drivers frequently had female partners who were (claimed to be) passive users. A similar gender dynamic was reported in an older paper by Mennicken et al. (2012) [162]. Though we cannot generalize this dynamic to the entire smart home user population, in light of gender differences in other technology domains (e.g. software usage [47, 48, 201], ambient belonging [166, 57], and domestic technology [58, 200]), we suggest that future work (1) explicitly study the role of gender in smart homes, (2) situate these findings in the broader study of gender, domesticity, and technology, and (3) develop designs to make smart devices more accessible to a diverse population.

3.5.2 Design Recommendations

Design to Minimize Power Differences

Smart home technology designs can and should take a role in minimizing the power differences among users in the home.

Analog Control While automation and remote control are great benefits of smart devices, this functionality is often not available to co-occupants who do not have phones, who prefer analog control, or who are dealing with an Internet or other failure. When a device stops working (as in Section 3.4), passive users who do not know how to troubleshoot the issue have to rely on either the smart home driver or analog controls (if available). Smart device manufacturers should thus recognize the important of backwards compatibility and design for it as much as possible. For example, smart devices should include easy-to-use mechanical switches and controls, at least for basic features (e.g., turning lights on and off). Smart outlets could perhaps alert users (via sound or light) attempting to manually control devices plugged into it when the smart outlet is off (and thus power is, perhaps unexpectedly, not flowing to the device).

Account Creation Smart home designers should support users in considering the entire household in the account creation process. For example, when on-boarding a new installer, smart home related applications should ask if there are other people in the home and streamline the process for their device access as well. The Nest app already does so, and we recommend that other companies follow. At the same time, developers should aim to require the minimum possible prerequisites for users to engage with their smart devices and applications. For example, we note that Apple Home requires users to have iCloud accounts and iOS 11.2 or later (i.e., iPhone 5 or later) [24], which may be a barrier for users with older devices.

Consider Different Relationship Types More generally, designers should consider the variety of relationships that may exist between smart home installers or driver and other occupants, or in non-traditional home units, including partners, roommates, children and parents, older adults, landlords and tenants, people in potentially abusive relationships, etc.

For example, consider a landlord who installs smart devices in a renter's apartment. What kind of control should tenants have over whether and what data is collected via these devices, the remote access by the landlord, and whether smart devices are installed at all? Some of these questions may be legal questions, but smart home device designers should consider them as well—e.g., considering how a "tenant mode" might differ from an "owner mode".

Smart homes also affect *non*-occupants of the home, including household employees (e.g., childcare providers, cleaners, and tradespeople) and guests. Designers should consider possible interactions with these people, who may need temporary access to devices or have privacy concerns, or from whom occupants may wish to protect their own privacy. For example, with devices that collect information for future use, such as Spotify through a voice assistant, a visitor mode could allow guests to use the device but not record their command and music history, supporting both owner music recommendations and non-occupant privacy.

Designing for Long-Term Changes

As smart home devices become more widely adopted, we may expect that they become long-term fixtures in people's homes , and we urge smart home designers to consider the long-term use of their devices and platforms.

Occupants Changing Some smart home fixtures may remain physically with a home when people move, such as smart outlets or thermostats. Since many people move, these devices should have built in functionality that allows old accounts and data to be easily deleted or migrated.

Some devices, such as the Nest and Ecobee thermostats, already have this functionality, and we recommend that other devices follow their lead. However, we note that one of our participants reported finding a previous tenant's account still connected to the Nest thermostat, suggesting that the usability or discoverability of this function could still be improved. For example, a possible solution with improved usability might involve smart devices automatically detecting changes that suggest a new tenant and prompting them locally—or the previous user remotely, e.g., via email—to reset the device and delete old data and accounts.

Handling occupant or other relationship changes correctly in general may be challenging, and designers should consider the full range of possible circumstances. For example, consider the August smart lock. To reset it, one must submit proof of purchase and the lock serial number to the company, who will contact the old owner to validate that the reset was intended. While this design choice prevents an attacker from resetting a lock to gain access to the home, it can also raise security concerns when the former owner *is* an adversary who may wish to prevent the lock from being reset (e.g., a former spouse in an abusive relationship).

Relationships Changing Even if the occupants of a smart home do not change, the relationships between the people living there might change over time. For example, as

children grow up, the changes in parent-child relationships can significantly impact smart home interactions and may require fundamental changes to how the smart home is setup and managed. While some prior work brings up the importance of designing devices for seasonal changes in a child's life [74], we want to call attention to how the change in trust and power between a parent and child might affect smart device usage as people grow older.

3.6 Limitations and Future Work

A major limitation of our study is that all except two of our participants were smart home drivers. Thus, while we can report on the perspectives of smart home drivers, our results do not fully reflect the experiences of passive users, who may have additional or more serious concerns than those raised in our interviews. For example, the lack of passive users in our sample may explain the limited concern about privacy or power imbalances in our findings. We advocate that future work study (1) passive users in significantly more depth to understand their perspectives, and (2) how to better engage and provide information to passive users, should they need or want to use smart devices.

Future work should also consider the concerns of children in smart homes, as well as how interactions with smart homes change over a longer period of time than a few weeks. For example, at what age do children gain the agency to have a say on smart devices in their personal spaces? What will be the longer-term privacy perceptions of children who grow up in smart homes surrounded by devices like cameras and digital assistants?

We also recommend that future work focus on designing and evaluating the technologies themselves: for example, evaluating the usability and discoverability of important device functions, such as account and data deletion and resetting (e.g., for when a new tenant moves in).

3.7 Conclusion

As smart devices move beyond early adopters and become integrated into the longer-term infrastructure of users' homes, we must critically consider how these technologies interact

with complex and changing human relationships, particularly relationships where there is a power imbalance. To study potential conflicts around smart homes, we conducted a mixed-method qualitative study of interactions and tensions that occur between people sharing a smart home.

Our results paint a picture of households where smart home use reflects existing relationship dynamics and power structures in homes (e.g. parent and child), and use that creates power imbalances. For example, smart home drivers tend to have more expertise access to functionality and data than passive users. We make recommendations for designers and researchers to help minimize these differences between co-occupants, to consider different relationship types, and to design for long-term use as children grow up and people move.

In addition to design recommendations, this work shows the importance of considering differential power relations with security and privacy, as mentioned in Chapter 1. Those with more power, whether because they were the smart home driver or because of their relationship position (e.g., parent), had more agency to make smart home privacy decisions and access control decisions for others in the household. Their decisions directly affect the privacy and security of others.

Chapter 4

USABLE SEXURITY: UNDERSTANDING DIFFERENTIAL SECURITY CONCERNS AND HARMS AROUND SEXTING

Intimate communications is another context in which marginalized communities face worse risks. For example, prior research has noted that women and non-binary are more likely to be threatened with or experience non-consensual image sharing (NCII). Feminists have argued that women are shamed for having sexual agency as a form of social control. This stigma around women expressing sexual desire leads to real consequences for leaked intimate messages, like potentially losing one's job. This risk means women are less free from consequences than men for NCII; they are less free to send intimate messages; they have less agency in this context.

With the understanding that some groups (e.g., women, non-binary folks, queer women, women of color [63]) face disproportionate risk with intimate communications, supporting sexting security is an equity issue. To that end, this chapter explores various users', particularly LGBTQ users', security concerns and mitigation strategies around intimate communications.

The material in this chapter first appeared as: Usable Sexurity: Studying People's Concerns and Strategies When Sexting. Christine "Chris" Geeng, Jevan Hutson, and Franziska Roesner. 16th Symposium on Usable Privacy and Security (SOUPS), August 2020 [97].

4.1 Introduction

Sexting is a common sexual behavior for adults in the United States, as technology has allowed greater ease of sharing and accessing sexual media [117]. The rise of ubiquitous mo-

bile devices has supported sexting practices—for example, the major social media platform Snapchat was founded based in part with the idea of making it less risky to sext [93], and many other apps exist that aim to provide privacy protections for interpersonal communications.

While sexting has become common, much of psychology work has characterized it as deviant behavior [195]. This perspective leaves out the opportunity to understand and design for sexting as a normal human behavior. Sexting *does* carry real risks—not due to an inherent immorality, but because sexts can be abused. For example, 1 in 25 Americans has been a victim of "revenge porn" (in which sexual imagery of someone is distributed without their permission) or threats of it. Women below 30 are more likely to be targeted than men or older women, and queer individuals are more likely to be targeted than heterosexual individuals [138]. But sexting also provides significant benefits, enabling self-expression and intimacy building in consensual relationships [64].

Thus, in this work, we engage with sexting as a normal adult practice and study people's technology-related concerns and practices related to sexting. Our work builds on and complements a call from the law and policy community to "conceptualize sexual privacy clearly and to commit to protecting it explicitly" [64]. We aim to understand how people navigate and conceptualize issues of privacy and security, and begin to articulate a framework for future research and development in usable security and privacy for sexting. We ask the following research questions:

1. *RQ1: Practices and Experiences.* What are people's general practices and experiences with technology-mediated sexting?

2. *RQ2: Concerns.* What are people's computer security concerns and threat models related to technology-mediated sexting?

3. *RQ3. Mitigations.* What are people's (technical or non-technical) mitigation strategies for managing these concerns?

We present results from an anonymous online survey of adults who have sexted at some point in their lives ($N = 247$). We asked questions about with whom, how often, and on what platform people sext, as well as about their concerns and mitigation practices. We find significant concerns around both sending sexts (e.g., that they will "get out" somehow, be misused in specific ways, or be seen accidentally by the wrong person) as well as receiving them (e.g., receiving unsolicited sexts or shoulder-surfing of solicited sexts). We further find that people rely heavily on non-technical strategies for mitigating these risks, including conscientiously establishing trust and social contracts with their sexting partners—suggesting a potential role for sexting platforms in helping scaffold or support these social contracts.

We close by making design recommendations and identifying opportunities for future research, grounded in Citron's legal sexual privacy framework to support individual autonomy, intimacy, and equality around sexting. Our work lays a foundation for considering and supporting security and privacy for sexting as a normal behavior among technology-using adults.

4.2 Motivation and Related Work

We define "sexting" as the technology-mediated interpersonal exchange of sexual media, including flirtatious or sexually explicit text or emojis, and nude or semi-nude photos and videos. In this section, we survey prior scholarship on sexting and usable security, identifying gaps that motivate our work.

4.2.1 Scholarship on Sexting

Sexting has become a common practice: Herbenick et al. found that 27% of adult women and 24% of adult men in the United States sent nude or semi-nude photos of themselves to someone [117], and Madigan et al. found that 14.8% and 27.4% of teens send and receive sexts, respectively [145].

Academic Framing Despite the pervasiveness of sexting, much of the academic work has focused on youth and young adults [83, 113, 195]. Furthermore, early literature on sexting treated it as a high-risk, deviant behavior, rather than an important part of adult social life that is just as normal as not sexting [82, 136]. Döring calls for an approach to sexting that acknowledges both "vulnerability and sexual agency" [82].

Research on youth has pointed out important concerns, such as adolescents feeling pressured to sext due to the erroneous belief that "everyone is doing it" [234, 142]. While youth and adult sexting both share some of the same risks and questions, it is important to also study the adult risk landscape. Our work seeks to better understand how adults (not just students) sext, from a perspective that views sexting as normal (and even important) intimate communication. Research scholarship on consensual sexting behavior has highlighted its positive role in relationship satisfaction [46, 80, 214], and that the affordances of sexting may lead to stronger sexual norms around explicit communication and consent [112]. Other work highlights potential issues that can arise with sexting, such as if the content is distributed without authorization, or if it occurs under pressure or as the result of coercion [62, 219, 22].

Mitigation Strategies Our study expands on prior work on sexting concerns and mitigations. Sex education researchers have studied how to teach youth about safe sexting and navigating consent, coercion, and digital footprints [181, 133]. Renfrow et al. found that college students minimized perceived risks through strategies around controlling sexting content, including 'keeping it fun' (avoiding more vulgar terms), limiting explicitness, and creating plausible deniability [195]. Amundsen [22] conducted qualitative interviews with women about the role trust has as a mitigation strategy for non-consensual sext sharing, and how the responsibility of mitigating risk may disproportionately fall upon victims, which are themes reflected in other work [227]. These prior studies do not deeply consider the role of technology (which can both create new concerns and support new mitigations) in sexting. In this work, we take a computer security point of view.

Beyond academic research, there are numerous applications that aim to (or are com-

monly used to) support sexting, as well as online guides for how to sext "securely". For example, Vice [150] lists guidelines including: get consent and set expectations, check for identifying details in photos, turn off services that automatically backup photos, wipe photos of EXIF metadata, and choose a communication app based on one's concerns. In terms of applications, Snapchat is popular with disappearing messages (which disappear quickly from the user interface, and are deleted from Snapchat servers within 30 days [10]), among other features such as screenshot notifications and a password-protected photo album. Other sexting guides list encrypted messaging platforms such as Signal, Whatsapp, and Facebook Secret Messenger. Less well-known examples include Kaboom (which allows users to send a disappearing message through a link, so that the receiving party can see the message without installing Kaboom) and Confide (a messaging app that has disappearing encrypted messages and screenshot notifications).

4.2.2 Sexual Privacy Framework

Legal scholar Danielle Citron argues that sexual privacy—"the social norms (behaviors, expectations, and decisions) that govern access to, and information about, individuals' intimate lives"—is a privacy value of the highest order because it is central to sexual agency, intimacy and equality: "[w]e are free only insofar as we can manage the boundaries around our bodies and intimate activities" [64]. Citron outlines how sexual privacy is foundational to (1) securing autonomy, (2) enabling intimacy, and (3) protecting equality.

While other privacy frameworks exist, such as contextual integrity [172], we find sexual privacy to be most appropriate for framing our study, as it forefronts the existence of unequal vulnerabilities (something that norm-based privacy theory does not do [158]). We briefly summarize these properties here, helping to motivate why protecting sexual privacy is crucial. We then place our results and recommendations in terms of this framework in Section 4.5.

Securing Autonomy Citron and others argue that sexual privacy is fundamental to the exercise of human agency and autonomy [64]; it is what allows individuals to manage the

boundaries of their bodies and their intimate lives [18, 155]. This autonomy, in turn, is viewed as fundamental to individual self-development and identity formation (who we are and who we might be in the future) [165, 33, 155, 193]

Enabling Intimacy Scholars have also argued that sexual (and other) privacy is critical to cultivating interpersonal intimacy, affection, and trust [64, 197, 90]. Indeed, research demonstrates that sexual privacy is key to the formation, maintenance, and growth of intimate relationships [19, 230, 194, 38, 92]. Intimacy is associated with important consequences for individual personal welfare, including heath, well-being, community attachment and sexual sociality [102]; research has further established a positive relationship between sexual activity and such outcomes as lifespan [179] and overall happiness [37].

Protecting Equality Sexual privacy also implicates issues of equality, justice, and power [75, 199], as women, sexual minorities, and nonwhites continue to bear the disproportionate burden of sexual privacy harms, such as surveillance, harassment, and abuse [64, 208, 209, 63, 202]. More broadly, political theorists argue that intimacy is a matter of justice, as access to access to intimacy is critical to accessing primary social goods such as wealth and self-respect [64, 28]. Scholars also underscore how the intimate sphere, both digital and non, is inextricably tied to relations of power [129, 63, 175, 85, 32, 33] and has historically been a key determinant of social and economic welfare [85, 28, 103].

4.2.3 Scholarship in Usable Security & Privacy

Finally, our work is situated in the broader space of usable security and privacy research, particularly studies on how people navigate sharing information in interpersonal relationships, such as account and device sharing in relationships [180, 151], online dating [65], social media [147], and human trafficking [**?**]. Freed et. al and others have studied how technology and information shared during the beginning of a trusting relationship gets abused when that turns into intimate partner violence [88, 89, 152]. These various settings surface both

overlapping lessons (e.g., how changes in relationships over time lead to different security or privacy vulnerabilities [140], such as a parent giving a child more privacy as they grow older [98]) as well as distinct challenges for different populations. At the highest level, these works reflect that threat modeling and design must follow a socio-technical approach, considering the properties of technology, how people use it, how people interact with each other, and societal expectations for such behavior.

4.3 Methods

We designed an anonymous online survey, using both close- and open-ended responses, to investigate the technology-related sexting behaviors and concerns of adults.

4.3.1 Ethical Considerations

Our study was reviewed and determined exempt by our institution's IRB. Given the potentially sensitive nature of our topic of study, we did not collect any identifying information from participants. Only participants who indicated that they were 18 years old or older were able to complete the survey. The opening paragraph to the survey emphasized that sexting is a common practice and that we as researchers are not taking a judgemental stance on it. The majority of questions were optional, including the choice "Prefer not to say". Participants could opt out of allowing their (anonymous) quotes from free-response answers to be used in this publication. The quotes we include in our results were chosen to illustrate patterns of behavior, rather than any individual's unique or potentially identifiable situation.

4.3.2 Recruitment

To recruit participants, we posted links to the survey on our personal Facebook, Twitter, and TikTok accounts. To widen recruitment beyond our personal networks, we distributed our survey via physical fliers in a major U.S. city and posted online to Reddit "subreddits" (e.g., /r/sex). Because prior literature often fails to capture the nuances of sexting among

Gender		Sexual Orientation		Age Range		Intimacy Status	
Male	30.36%	Straight	46.96%	18-24	52.23%	Single	25.10%
Female	61.54%	Questioning	2.02%	25-34	37.25%	Dating	35.22%
Non-binary	9.72%	Gay	8.10%	35-44	6.07%	Engaged	3.24%
Prefer not to say	0.81%	Lesbian	7.29%	45-54	3.24%	Married	10.53%
Self-describe:	1.21%	Bi/Pan	23.08%	55-64	1.21%	Divorced	2.02%
		Queer	6.48%			Friend-with-benefits	16.60%
Trans	5.67%	Asexual	1.21%			Casual sex	11.74%
Cis	89.47%	Prefer not to say	1.62%			Casual dating	16.19%
Questioning	3.24%	Self-describe:	3.24%			Prefer not to say	1.62%

Table 4.1: Demographics of 247 survey participants included in our analysis. Gender and intimate status categories were not mutually exclusive, so participants could use multiple labels to describe themselves.

sexual and gender minority communities (e.g., [78]), we also recruited specifically from queer social media groups and apps; this may explain why we sample more non-straight identifying participants than reflected in the United States population [171]. Four $20 gift cards were provided to random participants.

Upon beginning the anonymous online survey and after indicating their informed consent, participants were directed to questions that established whether they were at least 18 years old and whether they have ever engaged in sexting. If participants were under the age of 18 or indicated never having participated in sexting, they were dismissed from further data collection and analysis. We excluded people who had not sexted before because our research

Relationship Practice	
Monogamous	77.33%
Polyamorous	16.19%
Prefer not to say	6.48%

Table 4.2: Participants' relationship practice ($N = 247$).

questions focus on existing behaviors.

4.3.3 Procedures

We chose an online survey method to allow us to capture a broad population of people who sext [169]. We were especially interested in engaging with individuals over 18 because existing literature skews heavily towards youth and adolescent sexting practices [195]. To ensure that our research reflected the full constellation of gender identity, we followed Klaus et al.'s HCI Guidelines for Gender Equity and Inclusivity [205] in designing our demographics questions, which were asked at the end of the survey.

We asked three classes of questions in our survey, corresponding to our three research questions: (1) questions about general technology-enabled sexting practices; (2) questions about sexting-related concerns; and (3) questions about mitigation strategies to manage those concerns. The full survey instrument can be found in Appendix 7.2.1.

For questions related to concerns around sending or receiving sexts, we first asked an open-ended free response version, followed by a multiple-choice version. The goal was to first elicit concerns naturally, without priming participants about what they could or should be concerned about.The multiple choice options were based on our own hypotheses as well as informed by an existing survey related to concerns among university students around sexting [195].

For participants who completed the survey, they could opt-in to submitting their email to be entered into a raffle for a $20 gift card. Their email was not linked to their survey

data.

4.3.4 Data Analysis

We collected a total of 330 finished surveys, 249 with respondents who selected that they were at least 18 years old and had sexted before. Three researchers went through the open-ended data to look for disingenuous (e.g., joke) answers; we removed 2 respondents and completed our data analysis based on the remaining 247 responses.

For each open-ended free-response question, three researchers independently inductively coded those questions before discussing and agreeing on a set of qualitative codebooks (a separate codebook for each open-ended question). For questions where we asked an open-ended question followed by a similar multiple choice question, we incorporated the multiple choice options into our codebooks where appropriate. With the finalized codebooks, two researchers independently recoded the open-ended responses. All open-ended responses could have been coded with multiple labels.

Following McDonald et al.'s guidelines on when to seek coding agreement [159], for open-ended questions with simple responses, we used only one coder. For open-ended questions with more complex responses that we discuss quantitatively (concerns about sending sexts, and managing sending concerns), two researchers double-coded all responses. We calculated Cohen's κ for inter-coder reliability, given that we had two coders and nominal data [161]. For concerns about sending sexts, we had a κ of "substantial" (0.61–0.80) to "almost perfect agreement" (0.81–1.00) for 91.3% of categories. For managing sending concerns, we had a κ of "substantial" to "almost perfect agreement" for 93.76% of categories. (More details on κ per category can be found in Appendix 7.2.3). We discussed discrepancies between coders for all codes until we reached a near-consensus.

We compare answers to some multiple choice questions across genders for statistical differences. Since respondents were able to select multiple genders, we evaluate differences with a test of multiple marginal independence, which is calculated using a modified Pearson's Chi-squared statistic and a bootstrapping method to estimate the sampling distribution [137].

We use a significance level of $\alpha = 0.05$. We report Cramer's V for effect size on a scale of 0 to 1 (with associations ¿ 0.10 indicating at least a small effect [66]). We discarded participants who selected "Prefer to self-describe" (2 respondents with different answers) or "Prefer not to say" for their gender, leaving us with three nominal variables (male, female, non-binary). Since we asked if participants were transgender in a separate question, we cannot distinguish that category with this analysis, and our results are limited in that respect.

4.4 Results

We now turn to our results, based on the 247 valid survey responses from sexting adults, and organized around our three research questions (general practices in Section 4.4.1, concerns in Section 4.4.2, and mitigations in Section 4.4.3).

Table 4.1 summarizes the demographics of our participants, and Table 4.2 summarizes the types of relationships they considered while reporting on their sexting behaviors.

4.4.1 Sexting Practices and Experiences

We begin by considering general sexting practices and experiences, to help provide context for the concerns, mitigations, and design recommendations that follow.

Sexting Frequency

We found that 58.6% (144) of our participants said they currently sext, 33.6% said they have sexted before and may again in the future, and 8.8% said they have sexted before but no longer plan to. Considering sexting medium (i.e., video, image, or text), we found that text-based messages and nude or semi-nude photos were the most common, compared to nude or semi-nude videos (which only half of our sexting participants reported sending or receiving). The results look similar for sending and receiving frequency, suggesting this behavior is reciprocal. Figure 4.1 breaks this down in detail.

For participants who reported not currently sexting (regardless of whether they plan to in the future), we asked them why they stopped sexting. This question was multiple choice

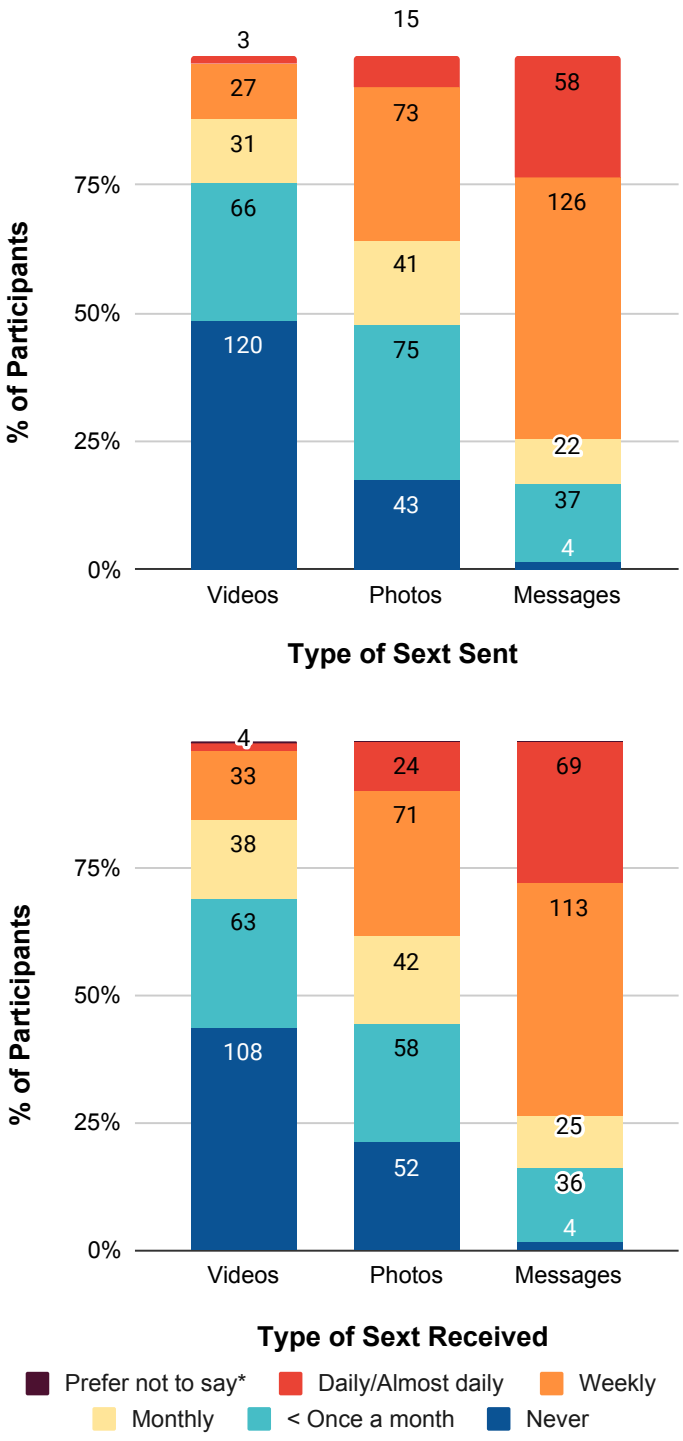

Figure 4.1: Participants reported how often they sent and received nude or semi-nude videos, photos, and sexual or intimate messages ($N = 247$). *1 person selected "Prefer Not To Say" for how often they received videos.

and optional; 106 participants responded. Of those, 45 said they stopped because they were no longer in a relationship with the person they sexted, and 31 said it was because they were no longer in a long-distance relationship. 28 said they were not interested, and 10 said they had had a poor experience. In a free-response follow-up question, out of the 10 people who selected having had a poor experience, 3 said sexting felt awkward, and 1 person said they were scammed.

For people who said they would sext again in the future, the majority marked their reason for stopping as no longer being in a relationship. For the people who said they would not sext again in the future, the majority marked their reason as not interested, with their explanations including "I honestly wasn't super into it", "no longer feels private", and "it felt like I was forcing myself into it".

Device and Platform Usage

Our participants primarily sext on their smartphone devices: 244 use their phone, 73 use their computer, and 16 use their tablet (with some using multiple devices, i.e., these responses are not mutually exclusive).

When asked about how they use social media to send sexting-related photos/video, the majority of our participants answered that they use Snapchat direct message (114; see Table 4.3 for the full breakdown). For other platforms, SMS had the highest usage (for sending photos/video) at 137 participants, possibly because it is a phone's default messaging app. (2 "Other" responses explicitly mentioned iOS Message, which respondents may have also counted as SMS.) "Other" responses included: Tumblr, Whisper, Kik, Skype, Reddit, Discord, Wired, Burner, email, and other dating sites. We do not have data about whether participants used these exclusively for sexting or also for other purposes. Considering sexual and intimate text messages, the distribution of platforms used looks similar to what we see for photos/video in Table 4.3

Some participants reported using platforms that explicitly include security- and/or sexting-related functionality. For example, Snapchat has disappearing messages, screenshot notifi-

Social Media Platform	**Direct Message**	**Private Post**	**Public Post**	**Story**	**Other**
Facebook/ Messenger	44	3	2	0	4
Twitter	13	6	2	0	1
Instagram	36	7	2	2	1
Snapchat	114	14*	3	1	1
Other	42	4	4	0	5

Table 4.3: Multiple-choice responses to what social media platforms and communication type that participants use to send/receive photos or videos ($N = 220$; this excludes participants who only send intimate text). *Snapchat has "private stories", not "private posts"; this wording error may have confused participants.

cations, and a password-protected photo album. Considering the more obscure platforms mentioned by participants: Burner provides a temporary new phone number that allows for communication while obscuring one's actual phone number, Wire is an end-to-end encrypted communication app, and Kik and Whisper tout themselves as anonymous social media services. We returns to people's uses (or non-uses) of these features in Section 4.4.3

Storing Sexts

We explicitly asked participants about their practices around storing their own and other people's nude or semi-nude images or videos (which we refer to by the shorthand "nudes" below). We note that these responses must be interpreted under the risk of social desirability bias: participants may have underreported socially undesirable behaviors, such as storing or sharing sexts without consent.

With respect to one's *own* nudes, we found that out of 247 responses, 130 (52.6%) said they stored nude or semi-nude photos or videos of themselves, 114 said they did not, and 3 said preferred not to answer. We find that storing nudes received from *other* people is even

Other Platforms		
SMS	137	62.27%
Whatsapp	38	17.27%
Grindr	19	8.64%
Tinder	11	5.00%
Telegram	10	4.55%
Signal	6	2.73%
OkCupid	4	1.82%
Hinge	3	1.36%
Kaboom	1	0.45%
Confide	1	0.45%
Other	28	12.73%

Table 4.4: Multiple-choice responses to what other platforms participants use to send/receive photos or videos ($N = 220$).

more common: among 234 participants who reported having received a sext and answered this question, 145 (62.0%) stated they have saved nude photographs or videos they received, 85 said they had not saved any, and 4 preferred not to answer.

For participants who store others' nudes, we asked additional questions about why and how they are saved (which may help explain why more participants' save other people's nudes than their own). In response to an open-ended question about why, most participants mentioned saving others' nudes for later use (e.g., nostalgia, to masturbate). Several participants mentioned saving to share media with friends, but none of those responses explicitly mentioned getting consent from the sender to share. Two people noted they saved content with no intention of sharing it, and 9 people thought it was assumed they would save a partner's photos. We note that 24 people *did* mention that they saved nudes with permission from sender (and 4 people mentioned they were even asked by the sender to save). In this

Reasons for Saving Received Nudes	
To use/look at later	80
Insurance	5
Saving is app default	5
Partner is away	4
Asked by sender to save	4
To share with friends/others	3
To be able to find more easily	2
Mutual saving	2

Table 4.5: Coded counts of participant open-ended responses to why they saved sexts sent to them ($N = 145$).

case, this number is a lower bound on how many participants received explicit consent to save nudes, since we did not specifically ask this in the question.

In the words of one participant:

> "I saved them because my girlfriend took the time to take a nice photo, just for me, and she's given me the OK to save them. When I miss her, it helps to look through a medley of sexual and non-sexual photos of her." – Male, straight, 18-24

In another question, we asked explicitly about whether senders knew that nudes had been saved by the participant. Out of 145 responses, 110 said that senders knew, 24 said some of the senders know, 7 said they do not know, and 4 preferred not to say. When we consider *how* nudes were saved, we note that only a small number of participants reported methods that explicitly aim to avoid knowledge by the recipient: 56% of participants directly stored to device, 37% took a screenshot, 5% (10) took a photo (presumably to circumvent screenshotting notifications, i.e., taking advantage of the "analog hole"), and 3% selected "Other": one respondent mentioned using screenshotting apps to prevent Snapchat screenshot notifications (e.g., Private Screenshots), and another mentioned saving to a private folder.

Plans for Received Nudes that are Saved		
Save them until asked to delete them	56	38.62%
Save them indefinitely	48	33.10%
Save them for some amount of time	27	18.62%
Other	13	8.97%
Prefer not to say	1	0.69%

Table 4.6: Single-choice responses from participants who said they save nudes sent to them for what they plan to do with them ($N = 145$).

For participants who save other people's nudes, 75 said they store on their device's photo storage (e.g., "Camera Roll"), 49 said a separate on-device album, 32 said a specific secret-keeping app (e.g., Snapchat's "My Eyes Only" folder, Vault, or an encrypted folder on a desktop/laptop computer), and 17 said online (e.g., Google Photos, Dropbox; some apps mentioned in the prior option are also online storage). Only 5 participants noted that their reason for saving is because this is the app's default behavior, but we suspect that this is an under-count, since many participants mentioned using SMS and other apps that automatically save content by default.

Out of the 145 participants who said they save other people's nudes (see Figure 4.6), most said they would save until asked to delete. For respondents who selected "Other" and "Save them for some amount of time", many explained that they might save until the end of the relationship, or save for time periods ranging from a week to years. One person mentioned they assume the photos would be automatically deleted when iPhone's cache is full, and another person mentioned that they have not thought that far ahead.

Overall, our results suggest common practice involves saving received sexts—not typically for nefarious purposes, and often (reportedly) with the consent and knowledge of the sender. Given these legitimate uses, a recommendation or platform-enforced policy of not saving received nudes would often be impractical and overly restrictive.

Sharing Sexts

We also asked explicitly about whether participants shared received sexts with others. Out of 247 responses, 32 said yes, 213 said no, and 2 said they prefer not to say. For yes answers, many people mentioned showing to friends or partners, and some mentioned sharing unsolicited photos for support and mockery. Some participants took measures to protect the privacy of the sext's creator, including getting explicit permission to share or anonymizing or otherwise editing the sexts—for instance, cropping and censoring identifying information.

4.4.2 Concerns around Sexting

We now turn to our participants' concerns around sending and receiving sexts. For both types of concerns, we first asked an open-ended question to elicit natural, non-primed concerns, followed by a multiple-choice question that allows us to evaluate the frequency of named concerns.

Concerns Around Sending Sexts

Table 4.7 shows participant concerns about sending sexts in response to our multiple choice question. The following concerns were most prevalent: "Sexts get around to other people" (93) and "Sexts used as blackmail" (83). Similarly, the most-used codes for the open-ended concern question (which, again, was asked before the multiple choice) was "Sexts will get out" (38) and "Shared/shown to others" (24). While some participants indicated only generic concern, others indicated a more specific threat model, specifying adversary (e.g., partner or platform) or consequence (e.g., impact on career or possible negative judgement). For example, one participant wrote:

> "We live in a society of prudes —I worry that things will leak and get out there and people will judge me for what I have shared with someone under the pretext that it was going to be private." – Non-binary, asexual, 25-34

Many fewer participants in the open-ended response mentioned "Sexts used as blackmail"

Concerns Sending Sexts		
Sexts get around to other people	93	75.00%
Sexts used as blackmail	83	66.94%
Receiver's devices will get hacked and the content will get out	78	62.90%
Receiver will intentionally share content with others	72	58.06%
Regret	58	46.77%
Sexting causes ridicule from others	40	32.26%
Not sure I sent it to the right person	38	30.65%
Bullying or harassment from others	29	23.39%
Unwanted attention	28	22.58%
Legal liability	25	20.16%
Sexting makes people feel led on used or misunderstood	24	19.35%
Damages relationships	19	15.32%
Conflicts at work	19	15.32%
Unwanted sexual contact	15	12.10%
Engagement with law enforcement	10	8.06%
Other	9	7.26%

Table 4.7: Multiple-choice responses to what concerns participants have when sending sexts ($N = 124$). This excludes 122 participants who send sexts but did not indicate that they have concerns around sending sexts.

(9), "Revenge porn" (8), or "Misuse" (11) as concerns, compared to the 83 responses to "Sexts used as blackmail" in the multiple-choice question; there is a similar discrepancy with the hacking concern. Participants may not have considered the multiple-choice concerns without being prompted to, or found the multiple-choice questions easier and/or less effort to answer.

Our open-ended question surfaced concerns we had not anticipated in our multiple choice options. The language "revenge porn", "blackmail", and "misuse" was used rather than "Bullying or harassment" (from the multiple choice question). Some responses also gave insights into participants' thoughts about potential adversaries: 10 respondents noted they were not concerned because they trusted their partner, and 3 noted they were not concerned because they trusted the app.

On the flip-side, 6 respondents mentioned not trusting the platform companies, and 3 respondents were concerned about bugs or vulnerabilities in the app. Other concerns not mentioned in the multiple choice options included deanonymization (7), recipient will save sexts (6), insecure network or cloud (2), photos will be modified (1), and images will be used to impersonate sender (1). Referring to both saving sexts and deanonymization concerns, one participant (male, gay, 18-24) wrote: *"People will save the photos. Specifically photos of my face and body together."*

In the open-ended questions, many responses were vaguely worded and did not specify the person or platform that somehow distributes or leaks their content. Such responses could be a reflection of vague or broad threat models in the mind of the participant, or of survey fatigue and the limitation of not being able to follow up for elaboration. To the extent that these responses suggest genuinely adversary-less threat models, they reflect Venema et al.'s findings, in which the responsibility of people who share explicit photos without consent is invisible in how the risks are described (e.g., "they [i.e., the photos] spread" or using the passive voice) [227].

Gender Differences for Sending Concerns Men were significantly less likely to be concerned about blackmail ($p = 0.02$, $V = 0.15$), with 22.97% of men, 38.82% of women,

Concerned about sexts being used as blackmail?

	No	Yes	Total
Male	57	17	74
Female	93	59	152
Non-Binary	15	9	24

Table 4.8: $N = 243$. N here and for Table 4.9 includes all participants who said they send sexts and who selected at least Male, Female, or Non-binary for their gender.

Concerned about sexts causing ridicule from others?

	No	Yes	Total
Male	69	5	74
Female	123	29	152
Non-Binary	20	4	24

Table 4.9: $N = 243$.

and 37.50% of non-binary individuals selecting being concerned (Table 4.8). Men were also significantly less likely to be concerned about ridicule ($p = 0.04$, $V = 0.15$), with 6.76% of men, 19.08% of women, and 16.67% of non-binary individuals selecting being concerned (Table 4.9). We did not see significant gender differences for other sending-related concerns.

Concerns About Receiving Sexts

Table 4.10 breaks down participant concerns about receiving sexts in response to our multiple-choice question. The greatest concern was over unsolicited sexts—a concern that is well-founded, given that out of 247 responses, 56% of people (138) said they have previously received unsolicited sexts.

Another major concern was shoulder-surfing, a concern for both receiving and sending sexts. One participant (female, lesbian, 18-24) wrote: *"I want a warning before. [I] do not*

Concerns Receiving Sexts		
Receiving unsolicited content	43	66.15%
Shoulder surfing	34	52.31%
My device will get hacked and their content will get out	29	44.62%
Not really the person I think it is	10	15.38%
Other	6	9.23%

Table 4.10: Multiple-choice responses to what concerns participants have when receiving sexts ($N = 65$). This excludes 185 participants who receive sexts but did not indicate that they have concerns around receiving sexts.

want to open a snap with a nude and have my grandmother sitting next to me. [I] must have warning in advanced."

Again, our open-ended question surfaced additional concerns, including the sender may escalate behavior/harassment (3), receiving a sext in an inappropriate context (2), being triggered(1), future regrets (1), receiving illegal material (1), and false accusations (1). There were 10 multiple-choice responses to concern over sender authenticity (i.e., being sure about the identify of the sender), versus only 1 response in the open-ended question.

Another concern was feeling forced to reciprocate the sext (4), i.e., forced to send back a sext or engage in other related behavior. For example:

> "I am concerned that by me receiving sexts, it gives off the impression that I am open to any sexual activity/interaction with the other party." – Female, straight, 18-24

> "I often feel coerced into responding via reciprocation and if I don't then the person will be angry." – Female, bi/pan, 24-34

Gender Differences for Unsolicited Sexts Women and non-binary individuals were significantly more likely to receive unsolicited sexts ($p = 0.005$, $V = 0.19$) and be concerned

		No	Yes	Total
Have you received an unsolicited sext?	**Male**	42	33	75
	Female	55	94	149
	Non-Binary	7	16	23

Table 4.11: $N = 243$. N includes all participants who selected at least Male, Female, or Non-binary for their gender.

about that ($p = 0.04$, $V = 0.15$). 63% of women, 69.5% of non-binary people, and 44% of men have received an unsolicited sext (Table 4.11), and 21.85% of 151 women, 20.83% of 24 non-binary people, and 9.33% of 75 men indicated that they were concerned about this.

Women were also significantly more likely to be concerned about shoulder-surfing ($p = 0.02$, $V = 0.15$), with 17.88% of 151 women, 6.67% of 75 men, and 8.33% of 24 non-binary individuals being concerned. These comparisons can be viewed in table form in Appendix 7.2.2. This result echoes the earlier finding that women are more likely to be concerned about negative judgement (ridicule) as a consequence of sending sexts. We did not see significant gender differences for other receiving-related concerns.

4.4.3 Mitigation Strategies

Finally, this section reports on participants' mitigation strategies for the concerns mentioned above, again elicited via both open-ended and free-response questions. We observed that participants mentioned both technical as well as significant non-technical mitigations strategies.

Technical Strategies

In both the open-ended question (34) and in the multiple choice question (57), participants mentioned that they manage concerns by picking a platform with specific features they want. The most common featured mentioned (23 in open-ended) was disappearing messages.

Concern Management Behavior		
Only sexting with people you trust	110	79.14%
Using disappearing messages (e.g., Snapchat, Instagram stories)	65	46.76%
Prior talks to set rules/boundaries	59	42.45%
Choose app with features you want	57	41.01%
Limiting how explicit the sext is	53	38.13%
Ensuring plausible deniability e.g. not including identifying marks in photo	51	36.69%
Password-protect or encrypt sexts	31	22.30%
Other	7	5.04%
No strategies to manage my concerns	5	3.60%

Table 4.12: Multiple-choice responses to what kind of actions people take to manage their concerns, both around sending and receiving sexts ($N = 140$).

(The most-mentioned disappearing message app was Snapchat, consistent with responses about platforms used for sexting.) Another feature often mentioned (and also supported by Snapchat) is notifications when the recipient takes a screenshot of a sent message or image. While these UI-based features may be sufficient to enforce privacy in most circumstances, we note that this mitigation feature alone would not be sufficient if someone is concerned about a receiver sharing supposedly ephemeral sexts. That there exist screenshot apps to circumvent notifications, and recall that 10 of our participants said they take photos to save nudes rather than screenshot them.

Other technical strategies mentioned include: having a passcode that protects access to an image, app, or device (e.g., Snapchat's password-protected "For My Eyes Only" photo album), explicitly deleting messages or media, using encrypted platforms such as Telegram or Signal, and using app or platform settings to ensure that notifications do not make the sexts

visible (e.g., to a shoulder-surfer). Some participants explicitly wrote about the threat model they considered when picking a platform. For example, the following participant specifically picks a platform with content deletion because they are concerned about shoulder-surfing:

> "Telegram has message & chat history delete functionality (and I'm most concerned about messages being *seen* on my device, not on the other person's device - I trust them)." – Non-binary, pansexual, 18-24

Many participants listed anonymizing sexts as a strategy (29 open-response, 51 in MC)—for example, cropping or blurring faces, or taking photos without identifying features within the frame. Only one respondent out of 20 mentioned being aware of potentially identifying locations in the photo:

> "Using Signal, not showing face, no identifying marks/locations, no posting public photos that correspond in time/place to explicit photos, no full nudity, only send images that if they would get out I could claim they were art photography or not of me." – Female, bisexual and queer, 25-34

No participant mentioned being concerned about EXIF data, image metadata that can compromise privacy and that some online safe-sexting guides recommend deleting [150]. (We note that some apps strip EXIF data automatically. For example, Signal strips EXIF data from photos taken within the app, based on the authors' testing and some anecdotal online sources [15], though not official Signal documentation).

Non-Technical Strategies

The most common mitigation strategy in both the multiple choice (110) and free-response question (54) was only sexting with someone the person knows and trusts. Communicating rules and boundaries (which includes asking the receiver to delete the photos) was also common (25 in free-response), whether the receiver is a long-term partner:

> "I sext with my partner whom I trust and we had several conversations about sexting before we started (when to delete photos, if we were at risk of revenge porning each other (we're not)), from there we talked about several different platforms and ultimately chose an encrypted platform. It's not completely safe but it's a calculated risk." – Female, bi/pan, 25-34

or someone the participant does not know as well:

> "I don't have extensive conversations with the people, but I'll say something like...'if I send this, don't show it to anyone else.' Usually it's a one time comment and when they agree to keep it to themselves, everything is on the table to share. I need to have a minimum level of trust with a person before I'll sext." – Female, bi/pan, 35-44

Other non-technical strategies included limiting the explicitness of the photo (24 in the free-response) and only sending content the participant would be comfortable appeared in public (3). Three people listed not sexting as their mitigation strategy: i.e., potentially feeling forced to forgo opportunities for building intimacy, as we discuss further in Section 4.5.

One participant mentioned acquiring collateral as a strategy—i.e., ensuring that the other person sends a photo first that they can save as "insurance", to discourage the other person from ever misusing their images. For example:

> "I save them because usually the person whom I have sent content to had saved mine in chat (Snapchat) or screenshotted them. So I save them as a precaution/insurance/leverage (if it comes to that)." – Female, straight, 18-24

Often, participants mentioned using a mix of technical and non-technical strategies. The particularly high prevalence of interpersonal trust and norms as a mitigation strategy points to an opportunity for platform design that can help create and support such norms, which we discuss further in Section 4.5.

Handling Unsolicited Sexts	
Block	82
Ignore	56
Ask them to stop/Confront	33
Delete message	15
Report to platform	8
Troll them	4
Change subject (keep talking)	2
Take screenshot	1
Stop using platform	1
Respond positively	1

Table 4.13: Coded counts of how participants respond to unsolicited sexts ($N = 138$).

Mitigations for Unsolicited Sexts

The previously discussed mitigation strategies are ones that can be deployed proactively. By contrast, receiving an unsolicited sext requires a reactive strategy. Table 4.13 summarizes coded open-ended responses to a question about how participants manage unsolicited sexts. Participants used both platform-supported mitigations (such as reporting or blocking senders) as well as ad-hoc, conversation-based approaches. While most participants do not engage with unsolicited sexts, some reported reacting by "trolling" the sender in response:

> "Don't pay it much attention. Sometimes mess with them a bit, tell them something like 'It won't let me open it (your pic) it keeps giving me an error message'. They spend ages checking their message settings, trying to resend it, and trying to explain to me how to open it. But usually just ignore and don't respond. Sometimes will have a short conversation and maybe a bit of a laugh about it." – Female, straight, 35-44

Also, 8 people mentioned that their behavior depends on if the behavior is repeated, and

4 people said their behavior depends on if they know the sender. For example:

> "It depends. When it someone I have never spoken to, I will usually screen grab it then delete it from the app – share it with someone who is complaining about their wonderful relationship. However, if it is someone I know and have met, it is more upsetting – and I will either message them about what I don't want, or stop talking to them altogether. Usually with a simple 'No.' and block it." – Non-binary, asexual, 25-34

4.5 Discussion

Our study captures a rich account of adult privacy and security behaviors around sexting and expands existing knowledge of how individuals navigate sexual privacy in the digital age. Through this work we aim to conceptualize usable sexual privacy and security clearly and commit to protecting it explicitly (echoing Citron [64]). To that end, we adopt and embrace Citron's framework of sexual privacy from legal scholarship [64]—particularly the values it embodies: security autonomy, enabling intimacy, and protecting equality—to ground both the discussion of our research's implications and directions for future research and development.

4.5.1 Securing Autonomy

Establishing Sexting Norms & Boundaries Sexual privacy is, at its core, about the "social norms governing the management of boundaries around intimate life" [64]. Our results surfaced the ad hoc ways in which people articulate and establish norms, expectations, and boundaries around sexting in order to mitigate sexual privacy harms. Critically, our research implicates the role of platforms in scaffolding the articulation and establishment of these norms. Indeed, developing levers to articulate and establish one's preferences with respect to sexting is arguably key to individual sexual agency and autonomy as well as to establishing trust and ensuring accountability. Yet scaffolding sexting norms raises serious questions about both platform and individual responsibility. We consider two ways

of scaffolding sexting norms that should be explored in future research and development: product/platform-level policy and user interface design.

First, platforms can establish product policies or community guidelines with respect to sexting. For example, community guidelines could contain language like "Make sure to ask others for consent before screenshotting images or messages in chat feeds" or "Receiving a sext does not obligate a response in kind". In such an approach, the platform plays a central role in articulating norms around sexting (which can in turn reduce user autonomy in some ways).

Second, platforms can leverage user interface design to better enable users to articulate their own preferences and expectations around sexting. For example, platforms could provide fixed disclosure options for users to express particular preferences. The gay dating and hookup platform Grindr already provides an "Accepts NSFW Pics" profile disclosure field where users can select "Never", "Not At First", and "Yes Please." Here, the platform plays a more co-constructive role with respect to sexting preferences and expectations.

On the other hand, platforms could provide open-ended disclosure options (similar to a free-form "About Me" field) for users to express more individualized preferences around sexting. Here, the platform allows norms to be driven by individual users rather than the platform itself. Having the latter free-form space would make more sense on a mixed-use messaging app (e.g., Snapchat) than having a specific disclosure field for sexts, as users may use their messaging profile to contact different people for non-intimate reasons.

Platform Management of Unsolicited Sexts Our research aims to understand and support individual actions and mitigation strategies towards sexual privacy and safety, but our results must be viewed in a broader societal context where sexting can be both empowering or disempowering [22]. On the negative side, unsolicited sexts are a major concern (and a disproportionate burden for women). While norm-supporting mitigations can help reduce some unsolicited sexts as discussed above, they cannot prevent explicitly malicious behavior. This issue is particularly challenging, because while people can take some proactive actions

to manage their concerns about sending intimate content (e.g., avoiding identifying features), they can only take reactive steps to manage unsolicited sexts (short of being forced to opt out of platforms entirely).

This threat model suggests that platforms may need to take a more proactive role in mitigating unsolicited and harassing sexual content, not only in response to user reports. This role could take the form of messaging affordance design: for example, not allowing photos to be sent unless both people in a conversation enable the feature. Platforms could also play a greater role in detecting and blocking certain types of content directly, as others have proposed and begun experimenting with [149]. However, this approach comes with significant challenges that future work must consider—e.g., how to integrate or balance content detection with end-to-end encryption, and how such a feature might interact with (in the U.S.) the First Amendment and a company's legal liabilities [173].

4.5.2 Enabling Intimacy

Existing Platform Affordances Our study surfaced a number of extant design practices that worked to preserve sexual privacy and enable intimacy. Important affordances that surfaced in our study include screenshot notifications, disappearing messages, and password protection for files. While these features are common on platforms like Snapchat, they do not pervade a variety of the other platforms or mediums people use (but are not necessarily designed) for sexting (e.g., Facebook, SMS, Grindr, Tinder). Our results suggest that these affordances are an important starting point for other platforms looking to account for sexting. We note that the design of these affordances can and should be informed by the real threat models of users like our participants. For example, while Snapchat has been criticized in the past for its disappearing messages not being truly secure [206], we note that even less-than-perfect security may be sufficient against the more common threat models involving violations (sometime accidental) by communication partners rather than company access or sophisticated external "hackers". (Though supporting stronger threat models is also crucial for some users, especially those particularly vulnerable to targeted attacks).

More generally, the focus of our work has *not* been on unpacking the technical properties of different platforms used by our participants. Our work lays a foundation for important future work to study these technical properties and to identify—and bridge—any gaps between the threat models they securely support and the threat models important to individuals engaging in sexting.

Designing for Storage One area of technical design that our results draw attention to is around storage. We found that large fractions of respondents save their own (52.6%) and others' (62.0%) nudes or sexual images—often for legitimate purposes and with consent — suggesting that platforms must design for this behavior as a norm rather than an indication of the intent to misuse the content. These findings shed light on the need to grapple with the digital footprint of sexting: who stores it, how and where is it stored, and how is it secured? Our findings suggest a variety of overlapping models, including storage on personal devices, storage in a file-sharing service (e.g., Google Drive), and platform-based storage (e.g., some dating and hook-up platforms, like Scruff, Growlr, and Jack'd, provide built-in "private photo" storage where images can be access-controlled and access-monitored). Participants sometimes used a storage strategy deliberately and sometime incidentally (e.g., storing one's own photos in the device "Camera Roll"). Different strategies support different threat models, and we recommend that both users and platform designers face these choices consciously.

Opting Out as a Last Resort Finally, while only a few people indicated not sexting as a mitigation strategy, we highlight that this decision relates to (or rather, hinders) enabling intimacy. First, abstaining from sexting is a valid behavior to alleviate sexual privacy risk as well as a valid boundary one might establish with respect to their intimate life. Second, however, if sexual privacy concerns are causing people not to sext, but there are other behaviors or design practices that *could* mitigate these concerns, then it is not the optimal outcome for people to feel like they have to choose to opt out of sharing sexual media. A

goal of sexting platform design or other interventions, then, should be to support positive sexting and not force people to opt out due to unmitigated risks.

4.5.3 Protecting Equality

Supporting prior work [78, 138, 63, 202, 228, 168], our results provide further evidence to suggest that women and sexual minorities are disproportionately burdened by certain sexual privacy risks—receiving more unsolicited sexts, feeling pressured to sext, worrying more about negative judgements (both for sending and receiving) and the potential misuse of their intimate content.

It is crucial that future work in this space further study such disparate impacts and take them into account when designing to mitigate potential risks with sexting.

Our results also highlighted the potentially generic threat models of many participants when asked to consider sexual privacy concerns without prompting. Many participants expressed vague concerns, often in the passive voice, about their sexts "getting out". Though these responses could be due in part to the survey methodology (where we could not follow up to clarify the vague responses, and participants might have opted to answer the question quickly rather than exhaustively), these results echo findings from prior work [227] and raise concerns that participants have internalized "victim-blaming" perspectives, shifting the responsibility away from untrustworthy partners and other actors who take advantage of normal sexting behavior. We recommend that future work dig deeper into these questions.

4.6 Conclusion and Future Work

Via an online survey of 247 adults who sext, our findings contribute to the field of usable privacy and security by expanding our understanding of how adults navigate sexting, using both technical strategies such as disappearing messages and non-technical strategies such as relying on trust. We show (similar to prior work) that men were less likely than women and non-binary individuals to be concerned about certain potential sexting risks, and less likely to receive unsolicited sexts. Placing our results in the context of the sexual privacy framework,

we suggest ways platforms can support autonomy, intimacy, and equality through platform affordances and policies.

Future work on usable sexual privacy and security should consider 1) how communication platforms can surface and scaffold individuals' norms, expectations, and boundaries around sexting, 2) how usable security can address the broader inequities in the experience of sexual privacy harms, and 3) how the technical properties of privacy-enabling affordances compare to user expectations and assumptions around the security and privacy implications of such features.

Finally, this work shows that women and non-binary people, who already have identities that are marginalized and are disempowered compared to other genders when facing sexual harms, face higher risks of sexual privacy violation. It is important for research on security and privacy to continue exploring how marginalized communities face disproportionate harms with technology compared to others, to ensure people have equitable access to safety with technology.

Chapter 5

EXPERIENCES OF U.S. LGBTQ+ FOLKS WITH ONLINE SECURITY, SAFETY, AND PRIVACY ADVICE

The queer community is a population that faces marginalization in the United States. Due to stigma around being gay or trans, queer folks are often at risk of facing homophobic and transphobic harms while existing on social media or existing while dating. This threat of harms decreases their agency and power to move through the world.

To support this marginalized population, in this chapter, I study where queer folks turn to for security, privacy, and safety advice, as well as their barriers to its efficacy or finding it. Additionally, I use the framework of intersectionality in analyzing my results because other axes of identity, along with queerness, affect my participants' experiences. My work

The material in this chapter first appeared as: "Like Lesbians Walking the Perimeter": Experiences of US LGBTQ+ Folks With Online Security, Safety, and Privacy Advice. Christine "Chris" Geeng, Mike Harris, Elissa Redmiles, and Franziska Roesner. USENIX Security Symposium, August 2021 [96].

5.1 Introduction

About 80% of American *LGBTQ+* (an umbrella acronym including lesbian, gay, bisexual, transgender, and queer) adults use social media sites [217], 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 [121, 203, 100], but also be a place of significant potential harm [203, 94, 221]. In this paper, and in line with

prior work [187, 81], 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 [186, 188, 190, 189, 86, 191], LGBTQ+ individuals face identity-based risks that straight and cisgender individuals do not [139, 77, 146]. 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" [35].

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.

5.2 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.

5.2.1 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 [8]. LGBT youth are often homeless because they are thrown out by their parents upon learning they are gay [8]. While U.S. law technically protects LGBTQ+ people in the workplace [143], 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 [16]. 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 [36, 77, 49, 95, 203], a problem more generally known as context collapse [148]. This can be especially stressful for transgender individuals navigating transitioning and coming out on social media [105, 183, 106]. To manage different audiences, individuals use affordances including multiple social media sites or accounts, private accounts, and granular post visibility [77, 49, 95].

Risks in online dating and sexting Over half of lesbian, gay or bisexual American adults have used a dating app [23]. Online dating can provide queer individuals connection [218] and a space to explore one's identity [77]. 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 [65]. 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. [117], and researchers have highlighted its positive role in relationship satisfaction [46, 80, 214]. Sexting also comes with risks, such as non-consensual sharing of intimate images, that have worse consequences for women and non-binary individuals [97, 138].

Other risks The prior sections are a non-exhaustive list of possible harms targeted towards queer individuals. Queer and trans activists [139], refugees [198], sex workers [157], 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 [204] for different threat models largely to other work. But we also touch on the importance of these overlapping identities in Section 5.2.2.

5.2.2 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 [35], e.g. but not limited to, race, gender, class, sexuality, and disability [71]. Here we define power as agency and access to resources [72], and power dynamics as "differences in ability to take action between parties" [231].

The reason we are explicitly looking at power is because lack of power reduces one's ability to resist, reduce, or prevent harm [231, 27]. 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 [63].

Intersectionality also helps us analyze "across domains of power" [35]: 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 [84] (interpersonal). Harm can come from institutions, as well as from other marginalized individuals [203, 231]. 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.

5.2.3 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 [91], people with visual impairments [115], sex trafficking survivors [**?**], refugees [207], and journalists [160]. 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.

5.2.4 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 [207, **?**]. Researchers have said that good security advice should be *effective, actionable,* and *understandable* [190, 191]. Yet, general security advice online is often inactionable, whether due to the cost-benefit trade-off not being worth it [118, 86], too much advice existing with no prioritization [190, 31], or that "the right advice might change over time with the attack landscape, new technology, and experience" [191]. And security experts and non-experts have differing opinions on what "good" advice is [130].

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 [188]. 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 [186].

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" [233]. Even amongst queer individuals, queer life experiences and concerns can be very different [216]. Security advice exists specifically for women [39], gay online dating [4], queer individuals using Instagram [185], and Black Lives Matter protesters [229] 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 [17]. 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.

5.3 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.

5.3.1 Interview Protocol

We developed an interview script to ask questions about:

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?

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

Table 5.1: 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).

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 7.3.1.

Advice Prompts We also gathered queer safety advice available online as prompts for participants to think about behaviors related to concerns they had (Appendix 7.3.2). 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

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 5.2: Participants self-reported their gender and sexual orientation.

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 [232], 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.

5.3.2 Participants

We recruited 14 queer participants diverse across age, race, disability, and economic and educational status (Table 5.1). 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 5.2. 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 [101]. Ten participants live in urban areas, three in suburban areas, and one in a rural area.

5.3.3 Data Analysis

We conducted thematic analysis on the transcripts, using primarily inductive coding [44]. First, two independent coders familiarized themselves with all transcripts [43]. Then they independently coded four interviews before discussing code choices and agreeing on an in-

termediate 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 [159].

5.3.4 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 [109, 210]. 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.

5.4 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.

5.4.1 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.

Asking community

Friends and family Echoing previous work [186, 189], 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.

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" [189].

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.

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 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 5.4.2.

5.4.2 Barriers to Finding and Following Advice

We detail difficulties participants encountered to finding security, safety, and privacy information, as listed in Table 5.3. While inconvenience was sometimes cited as the reason that advice did not work (as in prior work [118, 189]), our participants faced additional trade-offs as well.

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*

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 5.3: Participants mentioned different reasons for not adopting advice.

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 [110].

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).

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.

Advice would interfere with material livelihood

As we discuss more below, people's identities are multi-faceted. 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.

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 [186], as well as in decision-making in general [53]. 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 [49].

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 [189]), 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.

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 [191].

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." [12]. 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 [122]. This coping mechanism may also extend to culture-based threats [35], 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 5.5.2.

5.4.3 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 [105], 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 [106].

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 [36]. 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 [221]. 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 [203].

Examples of peer-to-peer harms included invalidating a specific identity (e.g., bisexuality [231] 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.

5.5 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.

5.5.1 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.

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 [79], 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 [191], 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 [229]. Furthermore, Reeder et al. noted technology and other factors change over time, so efforts to create fully consistent advice may find themselves quickly outdated [191].

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" [31].

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 [185]), 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 [111, 56].

Share emotional and communal support with advice

Communication research has pointed out that advice preceded by emotional support was considered higher quality [87]. Security clinic professionals provide emotional support as part-and-parcel of their service [223], which is necessary for clients facing intimate partner violence [224]. 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 [17]. 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 [13]. 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 [107, 108].

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 [34]. 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 [17, 210].

Communicate credibility

As prior advice research [190], credibility research [167], 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 prioritize business interests over user harm. Therefore it is important for third parties, like the Electronic Frontier Foundation [9], 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.

5.5.2 Takeaways for Security Research

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 [72].

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" [120].

3. Oppression (and harm) can come from interpersonal connections, culture, disciplinary structures, or institutions [35], 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 [69].

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 [233]). 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" [174]. 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 [192]. 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.

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 [147, 210]. Individual behaviors will not always work because a) the problems folks face may involve other people (e.g., networked privacy [147]), 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 [174, 115, 235], and that because privacy is networked, one person's disclosure decisions inevitably affect their entire social circle [148, 147]. 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 [13].

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 [239], privacy policy unreadability [156], sex worker safety [27], prisoner surveillance [177], undocumented immigrant surveillance [104], 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]).

5.5.3 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) [182]. 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 [21, 157, 26]. 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 [50]. Future advice research could incorporate theory outside security, e.g., the planned risk information seeking model [134].

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.

5.6 Limitations

This research scratches the surface of queer-intersecting identities that lead to other vulnerabilities (e.g. LGBTQ+ refugees [198], sex workers [144], HIV positive folks [141], victims of intimate partner violence [84], activists [139], and parents [36] as a non-exhaustive list) or different contexts (non-U.S. cultures and nationalities [198, 174]). 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 [114], 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 [139], and advice research with transgender folks specifically is also needed.

5.7 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.

Chapter 6

CONCLUSION

New Internet-connected technologies allow people to do things more quickly and conveniently—check who is ringing the doorbell at home on one's smartphone, send intimate messages to a loved one across the country, etc. Unfortunately these new affordances come with security, privacy, and safety risks, which are more pronounced for users who are oppressed or lack power in these technological contexts.

Therefore, this dissertation uses power relations as a frame of analysis in studying usable security questions: e.g., what are people's security, safety, or privacy concerns around a technology, and what are their mitigation strategies? By analyzing these research questions in three technological contexts—smart homes, sexting, and online security advice—my thesis highlights how it is necessary to study both the security needs for marginalized populations, as well as consider non-marginalized users who are disempowered within specific scenarios. It is important to research and advocate for both the safety of oppressed communities like LGBTQ users, as well as individuals who lose power when technology is introduced.

In terms of the latter, Chapter 3 looked at how smart homes with multiple users navigate privacy and control tensions of IoT devices, particularly when there are disparities of power: between spouses, parent and child, or the smart home installer and a passive user. More related to marginalized populations, Chapter 4 explored the sexting practices of users, particularly LGBTQ folks, as they navigate or accept security risks of sexts being seen by someone other than the intended recipient. With the understanding that LGBTQ folks may face worse security and privacy harms, Chapter 5 studied where LGBTQ individuals in the U.S. look to for security, safety, and privacy advice, and what prevents that advice from being effective, whether that is because of their queer identity or other intersectional identities.

My contributions to the field of security are:

1. Empirical results backing design and policy recommendations for supporting disempowered users of smart homes, intimate communications, and queer folks seeking security advice.

2. A case study on how to incorporate intersectionality as an analytic framework in usable security research. Intersectionality can explicitly lay out how different marginalized identities across age, race, gender, etc., affect one's threats and the risk and degree of harm they face. And this work showcases how situational security threats and mitigations are based on one's position and environment in life.

3. Demonstrating how even technology users who are not a part of marginalized communities may be subject to a power imbalances with others, and how that can lead to threats to their privacy and agency with technology.

Of course, power imbalances are not limited to the technological contexts or specific populations I study in my thesis. As the United States continues to introduce legislation in 2022 to restrict the agency of marginalized communities, such as punishing people with uteruses seeking abortions, or punishing parents who seek life-saving, gender affirming healthcare for their children, people will be in need of secure communication, privacy against third-party data collection, and safety in digital and physical spaces. And even among these groups, people oppressed across multiple axes, such as being an undocumented immigrant seeking healthcare, raises the risk of harm. It is important for the security community to continue researching security for marginalized groups, and consider how power relations and having less power changes what individual actions are available to a user under threat. By examining the power that institutional threats pose to users, the security field can advocate for justice at a systemic level with legislation, support of community organizations, and platform policy changes.

Chapter 7

APPENDIX

7.1 Smart Homes

	Gender	**Race**	**Age**	**House Members**	**Member Ages**
P1	Male	White	26	Girlfriend	26
P2	Male	Black	37	Mother	69
P3	Female	Asian		Boyfriend	26
P4	Male	White	34	Girlfriend, 2 dogs, cat	32
P5	Male	Asian	23	3 Roommates	25, 23, 26
P6	Male	White	38	Wife, daughter, son	37, 8, 4 months
P7	Female	Asian	38	Husband, 2 daughters, dog	44, 16, 10
P8	Male	White	29	Wife, daughter	26, 1
P9	Male	White	33	Wife, daughter	29, 4
P10	Male	Asian	17	Mother, father, sister	40s, 40s, 13
P11	Female	Asian	24	2 roommates	27, 24
P12	Male	Black	43	Wife, son, daughter	41, 13, 10
P13	Female	Asian	20	7 roommates	college “sophomores or freshmen”
P14	Male	White	30	Wife	30
P15	Male	White	44	Gf is over several nights a week	40
P16	Male	White	34	Wife, 2 children	35, 5, 3
P17	Male	White	37	Wife, daughter	37, 18 months
P18	Male	Asian	29	Wife, cat	29

Table 7.1: Participant demographics.

7.2 Intimate Communication

7.2.1 Survey Instrument

1. Are you 18 years old or over?

   ∘ Yes ∘ No

2. Have you ever sexted? That is, do you create, send, or receive sexually suggestive messages, or nude or partially-nude photos, through digital communications?

   ∘ Yes, I currently sext. ∘ No, I have never sexted. ∘ Yes, I have sexted before and may again in the future. ∘ Yes, I have sexted before but no longer plan to.

3. Why did you stop sexting? (Select all that apply.)

   ☐ No longer in a relationship with the person who I sexted with (please elaborate) ☐ No longer in a long-distance relationship ☐ Not interested (please elaborate) ☐ Poor experience (please elaborate) ☐ Other: ☐ Prefer not to say

4. How often do you send:

   (Options: Never, Less than once a month), Once a month, Once a week, A few times a week, Almost everyday, Multiple times per day, Almost hourly, Prefer not to say)

   Nude or semi-nude photos ∘ ∘ ∘ ∘ ∘ ∘ ∘ ∘ ∘ ∘

   Nude or semi-nude videos ∘ ∘ ∘ ∘ ∘ ∘ ∘ ∘ ∘ ∘

   Sexual or intimate messages (such as words or emojis) ∘ ∘ ∘ ∘ ∘ ∘ ∘ ∘ ∘ ∘

5. How often do you receive:

   (Options: Never, Less than once a month), Once a month, Once a week, A few times a week, Almost everyday, Multiple times per day, Almost hourly, Prefer not to say)

   Nude or semi-nude photos ∘ ∘ ∘ ∘ ∘ ∘ ∘ ∘ ∘ ∘

Nude or semi-nude videos ○ ○ ○ ○ ○ ○ ○ ○ ○

Sexual or intimate messages (such as words or emojis) ○ ○ ○ ○ ○ ○ ○ ○ ○

6. What social media platforms do you use to send/receive nude or semi-nude photos or videos? Select all that apply (or select nothing if you do not send this type of content).

   (Options: Direct Message, Private Post, Public Post, Story, Other)

   Facebook/FB Messenger, Twitter, Instagram, Snapchat, Other social media app:

7. What other platforms do you use to send/receive nude or semi-nude photos or videos? Select all that apply, if any.

   ☐ SMS ☐ Whatsapp ☐ Tinder ☐ Grindr ☐ Hinge ☐ OkCupid ☐ Signal ☐ Telegram ☐ Confide ☐ Kaboom ☐ Dust ☐ Other platforms (separated by comma):

8. What social media platforms do you use to send/receive sexual or intimate messages (such as words or emojis)? Select all that apply (or select nothing if you do not send this type of content).

   (Options: Direct Message, Private Post, Public Post, Story, Other)

   Facebook/FB Messenger, Twitter, Instagram, Snapchat, Other social media app: ☐ ☐ ☐ ☐ ☐

9. What other platforms do you use to send/receive sexual or intimate messages (such as words or emojis)? Select all that apply, if any.

   ☐ SMS ☐ Whatsapp ☐ Tinder ☐ Grindr ☐ Hinge ☐ OkCupid ☐ Signal ☐ Telegram ☐ Confide ☐ Kaboom ☐ Dust ☐ Other platforms (separated by comma):

10. What devices do you use to send/receive sexts? Select all that apply.

    ☐ Phone ☐ Tablet ☐ Computer ☐ Other

11. With whom do you send nude or semi-nude photos? Select all that apply.

    ☐ Partner ☐ Regular sexual hookup (purely sexual relationship) ☐ Casual date or one-time hookup ☐ Friend-with-benefits ☐ Friend ☐ Acquaintance ☐ New person online ☐ Other: ☐ Prefer not to say

12. With whom do you send nude or semi-nude videos? Select all that apply.

    ☐ Partner ☐ Regular sexual hookup (purely sexual relationship) ☐ Casual date or one-time hookup ☐ Friend-with-benefits ☐ Friend ☐ Acquaintance ☐ New person online ☐ Other: ☐ Prefer not to say

13. With whom do you send sexual or intimate messages (such as words or emojis)? Select all that apply.

    ☐ Partner ☐ Regular sexual hookup (purely sexual relationship) ☐ Casual date or one-time hookup ☐ Friend-with-benefits ☐ Friend ☐ Acquaintance ☐ New person online ☐ Other: ☐ Prefer not to say

14. With whom do you receive nude or semi-nude photos? Select all that apply.

    ☐ Partner ☐ Regular sexual hookup (purely sexual relationship) ☐ Casual date or one-time hookup ☐ Friend-with-benefits ☐ Friend ☐ Acquaintance ☐ New person online ☐ Other: ☐ Prefer not to say

15. With whom do you receive nude or semi-nude videos? Select all that apply.

    ☐ Partner ☐ Regular sexual hookup (purely sexual relationship) ☐ Casual date or one-time hookup ☐ Friend-with-benefits ☐ Friend ☐ Acquaintance ☐ New person online ☐ Other: ☐ Prefer not to say

16. With whom do you receive sexual or intimate messages (such as words or emojis)? Select all that apply.

☐ Partner ☐ Regular sexual hookup (purely sexual relationship) ☐ Casual date or one-time hookup ☐ Friend-with-benefits ☐ Friend ☐ Acquaintance ☐ New person online ☐ Other ☐ Prefer not to say

17. Do you or have you ever saved any of the nude photographs or videos you have received?

    ○ Yes ○ No ○ Prefer not to say ○ Not applicable

18. Why did/do you save them?

19. How do you save them?

    ☐ Directly store to device ☐ Screenshot ☐ Take a photo ☐ Other:

20. What do you plan to do with them?

    ○ Save them indefinitely ○ Save them for some amount of time (please indicate an estimate): ○ Save them until asked to delete them ○ Other: ○ Prefer not to say

21. Approximately how many nudes of other people do you have saved on your device?

    ○ None ○ 1 to 10 ○ 11 to 100 ○ 101+ ○ Prefer not to say

22. How do you store other people's nudes? Select all that apply.

    ☐ Device's photo storage: Camera Roll ☐ Device's photo storage: separate album ☐ Online (for example: Google Photos, Dropbox): ☐ Specific secret-keeping app (for example: Private Photo Vault): ☐ Other:

23. Does the person(s) who sent you the nudes know you've saved them?

    ○ Yes ○ Some of the senders know ○ No ○ Prefer not to say

24. Do you store nude or semi nude photos or videos of yourself?

    ○ Yes ○ No ○ Prefer not to say

25. Approximately how many nudes of yourself do you have saved?

    ∘ None ∘ 1 to 10 ∘ 11 to 100 ∘ 101+ ∘ Prefer not to answer

26. How do you store your nudes? Select all that apply.

    ☐ Device's photo storage: Camera Roll ☐ Device's photo storage: separate album ☐ Online (for example: Google Photos, Dropbox): ☐ Specific secret-keeping app (for example: Private Photo Vault): ☐ Other:

27. Do you share received sexts with people other than the sender?

    ∘ Yes (please elaborate how you share): ∘ No ∘ Prefer not to say

28. If you share other people's sexts digitally, do you digitally edit these sexts?

    ∘ Yes (please elaborate): ∘ No ∘ I do not share digitally ∘ Prefer not to say

29. Have you received sexts or nudes from people you did not want to receive them from?

    ∘ Yes ∘ No ∘ Prefer not to say

30. How do you manage receiving sexts or nudes from people you do not want to receive them from?

31. Do you have any concerns related to sending sexts?

    ∘ Yes (please elaborate below) ∘ No ∘ Prefer not to say

32. If you answered "yes" to the previous question, please elaborate here: What are your concerns related to sending sexts? Or if not, why not?

33. What concerns do you have about sending sexts?

    ☐ Sexts get around to other people ☐ Damages relationships ☐ Conflicts at work ☐ Legal liability ☐ Engagement with law enforcement (e.g police) ☐ Sexting causes

ridicule from others ☐ Unwanted attention ☐ Unwanted sexual contact ☐ Sexts used as blackmail ☐ Bullying or harassment from others ☐ Regret ☐ Sexting makes people feel "led on", "used", or "misunderstood ☐ Not sure I sent it to the right person ☐ Receiver's devices will get hacked and the content will get out ☐ Receiver will intentionally share the content with others ☐ Other

34. Do you have any concerns related to receiving sexts?

    ∘ Yes (please elaborate below) ∘ No ∘ Prefer not to say

35. If you answered "yes" to the previous question, please elaborate here: What are your concerns about receiving sexts? Or if not, why not?

36. What concerns do you have about receiving sexts?

    ☐ Not sure if it's really the person I think it is ☐ My device will get hacked and their content will get out ☐ Shoulder surfing ☐ Receiving unsolicited/non-consensual content ☐ Other:

37. If you don't have concerns about sexting, why is that?

    ☐ I've done something to manage my concerns ☐ I trust the people I sext with ☐ I trust the platform I use to sext ☐ I don't care about how people react to my nudity and sexual expression ☐ My sexts are already public ☐ I'm just not really worried about it ☐ Other:

38. Describe your level of concerns related to sending certain types of sexts.

    (Options: Not at all concerned, Slightly concerned, Somewhat concerned, Moderately concerned, Extremely concerned, N/A)

    Photo, Video, Text Based

39. Describe your level of concerns related to receiving different types of sexts.

    (Options: Not at all concerned, Slightly concerned, Somewhat concerned, Moderately concerned, Extremely concerned, N/A)

    Photo, Video, Text Based

40. You selected that you were concerned about the following when sending sexts: [input]. Do your concerns depend upon the type of person with whom you sext, the type of platform you use, or other considerations?

41. You selected that you were concerned about the following when receiving sexts: [input]. Do your concerns depend upon the type of person with whom you sext, the type of platform you use, or other considerations?

42. Do you do any of the following to manage your sexting concerns?

    ☐ Choose a platform with specific features you want ☐ Using disappearing messages e.g. Snapchat, Instagram stories ☐ Password-protect or encrypt sexts ☐ Prior conversations to establish rules and boundaries ☐ Ensuring plausible deniability e.g. not including identifying marks in photo ☐ Limiting how explicit the sext is ☐ Only sexting with people you trust ☐ I do not have any concerns ☐ I do not have any strategies to manage my concerns ☐ Other:

43. You selected that you use the following strategies to manage your sexting: [input]. Could you please elaborate?

44. Can we use anonymized quotes from your free-response answers in future research publications?

    ○ Yes ○ No

45. What gender(s) do you identify as?

☐ Male ☐ Female ☐ Non-binary ☐ Prefer not to say ☐ Prefer to self-describe:

46. Do you consider yourself transgender?

    ○ Yes ○ No ○ Questioning ○ Prefer not to say

47. What is your sexual orientation?

    ○ Straight ○ Questioning ○ Gay ○ Lesbian ○ Bi/Pan ○ Queer ○ Asexual ○ Prefer not to say ○ Prefer to self-describe:

48. Do you consider yourself polyamorous or monogamous (regardless of current relationship status)?

    ○ Polyamorous ○ Monogamous ○ Prefer not to say

49. Which racial background(s) do you identify as?

    ☐ Asian ☐ Black ☐ Latino ☐ Native American ☐ Pacific Islander ☐ White ☐ Prefer not to say ☐ Prefer to self-describe

50. What is your current intimate status? (Select all that apply)

    ☐ Single ☐ Dating ☐ Engaged ☐ Married ☐ Divorced ☐ Widowed ☐ Friends-With-Benefits ☐ Casual sex ☐ Casual dating ☐ Monogamous relationship ☐ Polyamorous relationship ☐ Prefer not to say

51. What is your age?

    ○ 18-24 years old ○ 25-34 years old ○ 35-44 years old ○ 45-54 years old ○ 55-64 years old ○ 65-74 years old ○ 75 years or older

52. What kind of location do you live in?

    ○ Urban ○ Suburban ○ Rural ○ Prefer not to say

53. Have you ever been in an IT/technology related job?

    ◦ Yes ◦ No ◦ Prefer not to say

54. I understand how to control or protect my personal data online.

    ◦ Strongly agree ◦ Agree ◦ Somewhat agree ◦ Neither agree nor disagree ◦ Somewhat disagree ◦ Disagree ◦ Strongly disagree

55. What is your education level?

    ◦ GED ◦ Some high school ◦ Some college/technical training ◦ Some graduate school ◦ Prefer not to say

7.2.2 Additional Data on Gender Comparisons

Tables 7.2 and 7.3 show the data on gender comparisons for two receiving-related concerns, discussed in Section 4.4.2. The N value for both tables includes all participants who said they receive sexts and who selected at least Male, Female, or Non-binary for their gender.

	No	**Yes**	**Total**
Male	68	7	75
Female	118	33	151
Non-Binary	19	5	24

Table 7.2: **Concerned about receiving unsolicited sexts?** $N = 242$

	No	**Yes**	**Total**
Male	70	5	75
Female	124	27	151
Non-Binary	22	2	24

Table 7.3: **Concerned about shoulder-surfing?** $N = 242$

7.2.3 Inter-Coder Reliability

Tables 7.4 and 7.5 show the breakdown of Cohen's κ for inter-coder reliability per code, discussed in Section 4.3.4.

Managing Sending Concerns	κ
Only sext with trusted/known person	0.94
Don't sext	0.66
Communicating/establishing rules and expectations	0.90
Limit explicitness	0.91
Anonymize sext (no face, tattoos, names, or location)	0.93
Ask person to delete	1.00
Acquire collateral	1.00
Passcode protect image/app/device	1.00
Disappearing messages	1.00
Explicitly deleting messages/chat/media	0.66
Encrypted platforms	0.62
Screenshot notifications	1.00
Only send stuff willing to go public	0.49
Platform choice/Platform affordances	0.88
Making sure notifications don't make sexts visible	1.00
Other	0.82

Table 7.4: Cohen's Kappa for codes for elaboration on management strategies for sexting concerns.

Concerns About Sending Sexts	κ
Impact career	1.00
Sexts will get out (Vague)	0.69
Sexts used as blackmail	0.87
Deanonymization	1.00
Sending to wrong person	0.94
Bug or vulnerability in app	0.50
Revenge porn	0.87
Hacking or stealing	0.92
Recipient will save sexts	0.83
End up online	0.73
Shared/shown to others	0.81
Seen accidentally by non-recipient	0.77
Recipient will misuse (Generic, Other)	0.73
Not concerned because trust partner	0.79
Not concerned because trust app	0.80
Not trusting companies	0.72
Access by government	1.00
Images will be used to impersonate sender	0.66
Accidentally posting publicly	1.00
Judgement from others (also: embarrassing)	0.76
Insecure network or cloud	1.00
Photos will be modified	1.00
Other	0.32

Table 7.5: Cohen's Kappa for codes for open-ended question, "What are your concerns related to sending sexts?"

7.3 Security Advice for LGBTQ Folks

7.3.1 Interview Protocol

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

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?

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?

7.3.2 Advice Probes and Sources

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

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

BIBLIOGRAPHY

[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. 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. 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] 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).

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

[10] When does Snapchat delete snaps and chats? (Accessed on 02/07/2021).

[11] WIPS 2021. Workshop on Inclusive Privacy and Security, https://inclusiveprivacy.org/workshops/wips2021.html. (Accessed on 06/02/2022).

[12] 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).

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

[14] Multiple users - can they all see each other?, October 2017. (Accessed on 08/20/2018).

[15] Signal removes EXIF data #7862, 2018. https://github.com/signalapp/Signal-Android/issues/7862.

[16] 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).

[17] 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. (Accessed on 02/17/2021).

[18] Irwin Altman. *The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding*. Brooks/Cole Publishing Company, 1975.

[19] Irwin Altman and Dalmas A Taylor. *Social penetration: The development of interpersonal relationships.* Holt, Rinehart & Winston, 1973.

[20] Amazon. Echo & alexa devices. https://www.amazon.com/b?node=9818047011 ref=ODS_v2_FS_AUCC_category. (Accessed on 08/13/2018).

[21] Tawfiq Ammari and Sarita Schoenebeck. Understanding and supporting fathers and fatherhood on social media sites. In *Proceedings of the 33rd annual ACM conference on human factors in computing systems*, pages 1905–1914, 2015.

[22] Rikke Amundsen. 'The Price of Admission': On Notions of Risk and Responsibility in Women's Sexting Practices. In Karen Lumsden and Emily Harmer, editors, *Online Othering: Exploring Digital Violence and Discrimination on the Web*, Palgrave Studies in Cybercrime and Cybersecurity. Palgrave Macmillan, 2019.

[23] Monica Anderson, Emily A. Vogels, and Erica Turner. 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).

[24] Apple. Use the home app on your iphone, ipad, and ipod touch. https://support.apple.com/en-us/HT204893, 2018. (Accessed on 08/03/2018).

[25] Noah Apthorpe, Yan Shvartzshnaider, Arunesh Mathur, Dillon Reisman, and Nick Feamster. Discovering smart home internet of things privacy norms using contextual integrity. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 2(2):59:1–59:23, July 2018.

[26] Hanna Barakat and Elissa M. Redmiles. Community Under Surveillance: Impacts of Marginalization on an Online Labor Forum. In *16th International AAAI Conference on Web and Social Media*, 2021.

[27] Catherine Barwulor, Allison McDonald, Eszter Hargittai, and Elissa M. Redmiles. "Disadvantaged in the American-Dominated Internet": Sex, Work, and Technology. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, CHI '21, New York, NY, USA, 2021. Association for Computing Machinery.

[28] Sonu Bedi. Sexual racism: Intimacy as a matter of justice. *The Journal of Politics*, 77(4):998–1011, 2015.

[29] Genevieve Bell and Paul Dourish. Yesterday's tomorrows: Notes on ubiquitous computing's dominant vision. *Personal Ubiquitous Computing*, 11(2):133–143, January 2007.

[30] Victoria Bellotti and Abigail Sellen. Design for privacy in ubiquitous computing environments. In *Proceedings of the Third Conference on European Conference on Computer-Supported Cooperative Work*, ECSCW'93, pages 77–92, Norwell, MA, USA, 1993. Kluwer Academic Publishers.

[31] Kristin Berdan. An evaluation of online security guides for journalists, 2021.

[32] Lauren Berlant. Intimacy: A special issue. *Critical inquiry*, 24(2):281–288, 1998.

[33] Lauren Berlant and Michael Warner. Sex in public. *Critical inquiry*, 24(2):547–566, 1998.

[34] Thérèse Bernier, Amika Shah, Lori E Ross, Carmen H Logie, Emily Seto, 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):e26085, 2021.

[35] Sirma Bilge and Patricia Hill Collins. Intersectionality. *Cambridge, UK: Polity*, 2016.

[36] Lindsay Blackwell, Jean Hardy, Tawfiq Ammari, Tiffany Veinot, Cliff Lampe, and Sarita Schoenebeck. LGBT Parents and Social Media: Advocacy, Privacy, and Disclosure During Shifting Social Movements. *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, pages 610–622, 2016.

[37] David G. Blanchflower and Andrew J. Oswald. Money, sex and happiness: An empirical study. *Scandinavian Journal of Economics*, 106(3):393–415, 2004.

[38] Edward J. Bloustein and Nathaniel J. Pallone. *Individual and group privacy*. Routledge, 2018.

[39] Violet Blue. *The Smart Girl's Guide to Privacy: Practical Tips for Staying Safe Online*. No Starch Press, San Francisco, CA, 2015.

[40] James Bohman, Jeffrey Flynn, and Robin Celikates. Critical Theory. In Edward N. Zalta, editor, *The Stanford Encyclopedia of Philosophy*. Metaphysics Research Lab, Stanford University, Spring 2021 edition, 2021.

[41] Nellie Bowles. Thermostats, locks and lights: Digital tools of domestic abuse. New York Times, https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html, 2018. (Accessed on 08/13/2018).

[42] Stephanie Brail. The price of admission: Harassment and free speech in the wild, wild west. *Wired_Women: Gender and new realities in cyberspace*, 1996.

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

[44] Virginia Braun and Victoria Clarke. Conceptual and design thinking for thematic analysis. *Qualitative Psychology*, 2021.

[45] A.J. Bernheim Brush, Bongshin Lee, Ratul Mahajan, Sharad Agarwal, Stefan Saroiu, and Colin Dixon. Home automation in the wild: Challenges and opportunities. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '11, pages 2115–2124, New York, NY, USA, 2011. ACM.

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

[47] Margaret Burnett, Anicia Peters, Charles Hill, and Noha Elarief. Finding gender-inclusiveness software issues with gendermag: A field investigation. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, CHI '16, pages 2586–2598, New York, NY, USA, 2016. ACM.

[48] Margaret M. Burnett, Laura Beckwith, Susan Wiedenbeck, Scott D. Fleming, Jill Cao, Thomas H. Park, Valentina Grigoreanu, and Kyle Rector. Gender pluralism in problem-solving software. *Interact. Comput.*, 23(5):450–460, September 2011.

[49] Matthew Carrasco and Andruid Kerne. Queer visibility: Supporting lgbt+ selective visibility on social media. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, pages 1–12, 2018.

[50] Donald O Case and Lisa M Given. *Looking for information: A survey of research on information seeking, needs, and behavior*. Emerald Group Publishing, 2016.

[51] Marta E. Cecchinato and Daniel Harrison. Degrees of Agency in Owners & Users of Home IoT devices. *Making Home: Asserting Agency in the Age of IoT workshop in CHI '17*, 2017.

[52] Pew Research Center. Privacy and information sharing report. http://www.pewinternet.org/2016/01/14/scenario-home-activities-comfort-and-data-capture/, 2016. (Accessed on 08/22/2018).

[53] Sun-Ki Chai. *Choosing an identity: A general model of preference and belief formation*. University of Michigan Press, 2001.

[54] Rahul Chatterjee, Periwinkle Doerfler, Hadas Orgad, Sam Havron, Jackeline Palmer, Diana Freed, Karen Levy, Nicola Dell, Damon McCoy, and Thomas Ristenpart. The spyware used in intimate partner violence. *Proceedings of the IEEE Symposium on Security and Privacy*, pages 441–458, 2018.

[55] Christine Chen, Nicola Dell, and Franziska Roesner. Computer security and privacy in the interactions between victim service providers and human trafficking survivors. In *USENIX Security Symposium*, 2019.

[56] Jay Chen, Michael Paik, and Kelly McCabe. Exploring internet security perceptions and practices in urban ghana. In *10th Symposium On Usable Privacy and Security (SOUPS)*, pages 129–142, 2014.

[57] Sapna Cheryan, Andrew N. Meltzoff, and Saenam Kim. Classrooms matter: The design of virtual classrooms influences gender disparities in computer science classes. *Computers & Education*, 57(2):1825 – 1835, 2011.

[58] Noelle Chesley. Families in a high-tech age: Technology usage patterns, work and family correlates, and gender. *Journal of Family Issues*, 27(5):587–608, 2006.

[59] Marshini Chetty, Richard Banks, Richard Harper, Tim Regan, Abigail Sellen, Christos Gkantsidis, Thomas Karagiannis, and Peter Key. Who's hogging the bandwidth: The consequences of revealing the invisible in the home. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '10, pages 659–668, New York, NY, USA, 2010. ACM.

[60] Eun Kyoung Choe, Sunny Consolvo, Jaeyeon Jung, Beverly Harrison, and Julie A. Kientz. Living in a glass house: A survey of private moments in the home. In *Proceedings of the 13th International Conference on Ubiquitous Computing*, UbiComp '11, pages 41–44, New York, NY, USA, 2011. ACM.

[61] Eun Kyoung Choe, Sunny Consolvo, Jaeyeon Jung, Beverly Harrison, Shwetak N. Patel, and Julie A. Kientz. Investigating receptiveness to sensing and inference in the home using sensor proxies. In *Proceedings of the 2012 ACM Conference on Ubiquitous Computing*, UbiComp '12, pages 61–70, New York, NY, USA, 2012. ACM.

[62] HyeJeong Choi, Joris Van Ouytsel, and Jeff R. Temple. Association between sexting and sexual coercion among female adolescents. *Journal of adolescence*, 53:164–168, 2016.

[63] Danielle Keats Citron. *Hate crimes in cyberspace*. Harvard University Press, 2014.

[64] Danielle Keats Citron. Sexual privacy. *128 Yale Law Journal 1870 (2019); U of Maryland Legal Studies Research Paper No. 2018-25*, 2019.

[65] Camille Cobb and Tadayoshi Kohno. How public is my private life? privacy in online dating. In *Proceedings of the 26th International Conference on World Wide Web*, pages 1231–1240, 2017.

[66] Jacob Cohen. *Statistical power analysis for the behavioral sciences*. Academic press, 2013.

[67] Combahee River Collective. The Combahee River Collective Statement. http://circuitous.org/scraps/combahee.html.

[68] Sunny Consolvo and Miriam Walker. Using the experience sampling method to evaluate ubicomp applications. *IEEE Pervasive Computing*, 2(2):24–31, April 2003.

[69] Sasha Costanza-Chock. *Design justice: Community-led practices to build the worlds we need*. The MIT Press, 2020.

[70] M. Courtney. Careless talk costs privacy [censorship digital assistants]. *Engineering Technology*, 12(10):50–53, November 2017.

[71] Kimberlé Crenshaw. Demarginalizing the intersection of race and sex: A black feminist critique of antidiscrimination doctrine, feminist theory and antiracist politics. *u. Chi. Legal f.*, page 139, 1989.

[72] Kimberle Crenshaw. Mapping the margins: Intersectionality, identity politics, and violence against women of color. *Stan. L. Rev.*, 43:1241, 1990.

[73] Alexei Czeskis, Ivayla Dermendjieva, Hussein Yapit, Alan Borning, Batya Friedman, Brian Gill, and Tadayoshi Kohno. Parenting from the pocket: Value tensions and technical directions for secure and private parent-teen mobile safety. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, SOUPS '10, pages 15:1–15:15, New York, NY, USA, 2010. ACM.

[74] Scott Davidoff, Min Kyung Lee, Charles Yiu, John Zimmerman, and Anind K. Dey. Principles of smart home control. In *Proceedings of the 8th International Conference on Ubiquitous Computing*, UbiComp'06, pages 19–34, Berlin, Heidelberg, 2006. Springer-Verlag.

[75] Judith Wagner DeCew. *In pursuit of privacy: Law, ethics, and the rise of technology*. Cornell University Press, 1997.

[76] George Demiris and Brian K. Hensel. Technologies for an aging society: A systematic review of "smart home" applications. *Yearbook of Medical Informatics*, pages 33–40, 2008.

[77] Michael A DeVito, Ashley Marie Walker, and Jeremy Birnholtz. 'Too Gay for Facebook': Presenting lgbtq+ identity throughout the personal social media ecosystem. *Proceedings of the ACM on Human-Computer Interaction*, 2(CSCW):1–23, 2018.

[78] Allyson Dir, Ayca Coskunpinar, Jennifer Steiner, and Melissa Cyders. Understanding differences in sexting behaviors across gender, relationship status, and sexual identity, and the role of expectancies in sexting. *Cyberpsychology, behavior and social networking*, 16, 05 2013.

[79] Paul Dourish, Rebecca E Grinter, Jessica Delgado De La Flor, and Melissa Joseph. Security in the wild: user strategies for managing security as an everyday, practical problem. *Personal and Ubiquitous Computing*, 8(6):391–401, 2004.

[80] Michelle Drouin, Manda Coupe, and Jeff R. Temple. Is sexting good for your relationship? It depends.... *Computers in Human Behavior*, 75:749–756, 2017.

[81] Brianna Dym and Casey Fiesler. Social norm vulnerability and its consequences for privacy and safety in an online community. *Proceedings of the ACM on Human-Computer Interaction*, 4(CSCW2):1–24, 2020.

[82] Nicola Döring. Consensual sexting among adolescents: Risk prevention through abstinence education or safer sexting? *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 8, 01 2014.

[83] Nicola Döring and M. Rohangis Mohseni. Are Online Sexual Activities and Sexting Good for Adults' Sexual Well-Being? Results From a National Online Survey. *International Journal of Sexual Health*, 30(3):250–263, July 2018.

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

[85] Elizabeth F Emens. Intimate discrimination: The state's role in the accidents of sex and love. *Harv. L. Rev.*, 122:1307, 2008.

[86] Michael Fagan and Mohammad Maifi Hasan Khan. 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)*, pages 59–75, 2016.

[87] Bo Feng. Testing an integrated model of advice giving in supportive interactions. *Human Communication Research*, 35(1):115–129, 2009.

[88] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. "A stalker's paradise": How intimate partner abusers exploit technology. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, CHI '18, New York, NY, USA, 2018. Association for Computing Machinery.

[89] Diana Freed, Jackeline Palmer, Diana Elizabeth Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. Digital technologies and intimate partner violence: A qualitative analysis with multiple stakeholders. *Proceedings of the ACM on Human-Computer Interaction*, 1(CSCW):1–22, 2017.

[90] Charles Fried. *An anatomy of values*, volume 2. HeinOnline, 2013.

[91] Alisa Frik, Leysan Nurgalieva, Julia Bernd, Joyce Lee, Florian Schaub, and Serge Egelman. Privacy and security threat models and mitigation strategies of older adults. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS)*, pages 21–40, 2019.

[92] Erich Fromm. *The art of loving: The centennial edition*. A&C Black, 2000.

[93] Billy Gallagher. How Reggie Brown invented Snapchat, February 2018. https://techcrunch.com/2018/02/10/the-birth-of-snapchat/.

[94] Lesbian Gay, Straight Education Network, et al. Out online: The experiences of lesbian, gay, bisexual and transgender youth on the internet. *New York, NY: Author*, 2013.

[95] Christine Geeng. LGBTQ privacy concerns on social media. In *Proceedings of the 2018 CHI Conference Workshops and Symposia on Human Factors in Computing Systems*, Montréal, Canada, 2018. ACM Press.

[96] Christine Geeng, Mike Harris, Elissa Redmiles, and Franziska Roesner. "like lesbians walking the perimeter": Experiences of us lgbtq+ folks with online security, safety, and privacy advice. In *USENIX Security Symposium*, 2021.

[97] Christine Geeng, Jevan Hutson, and Franziska Roesner. Usable sexurity: Studying people's concerns and strategies when sexting. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*, pages 127–144, 2020.

[98] Christine Geeng and Franziska Roesner. Who's in control? Interactions in multi-user smart homes. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, CHI '19, New York, NY, USA, 2019. Association for Computing Machinery.

[99] Google. Google home - smart speaker & home assistant. https://store.google.com/us/product/google_home, 2018. (Accessed on 08/13/2018).

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

[101] Mary L Gray. *Out in the Country*. New York University Press, 2009.

[102] Adam Isaiah Green. The social organization of desire: The sexual fields approach. *Sociological Theory*, 26(1):25–50, 2008.

[103] Adam Isaiah Green. Sexual capital and social inequality. *Introducing the New Sexuality Studies*, 272, 2016.

[104] Tamy Guberek, Allison McDonald, Sylvia Simioni, Abraham H. Mhaidli, Kentaro Toyama, and Florian Schaub. Keeping a Low Profile?: Technology, Risk and Privacy among Undocumented Immigrants. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems - CHI '18*, pages 1–15, Montreal QC, Canada, 2018. ACM Press.

[105] Oliver L. Haimson, Jed R. Brubaker, Lynn Dombrowski, and Gillian R. Hayes. Disclosure, Stress, and Support During Gender Transition on Facebook. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing*, pages 1176–1190, Vancouver BC Canada, February 2015. ACM.

[106] Oliver L Haimson, Jed R Brubaker, Lynn Dombrowski, and Gillian R Hayes. Digital footprints and changing networks during online identity transitions. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, pages 2895–2907, 2016.

[107] Julie M Haney and Wayne G Lutters. Skills and characteristics of successful cybersecurity advocates. In *Workshop Program at Symposium on Usable Privacy and Security (SOUPS) 2017*, 2017.

[108] Julie M Haney and Wayne G Lutters. "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)*, pages 411–425, 2018.

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

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

[111] Eszter Hargittai et al. Facebook privacy settings: Who cares? *First Monday*, 2010.

[112] A.A Hasinoff. How to have great sext: consent advice in online sexting tips. *Communication and Critical/Cultural Studies*, 13(1):58–74, 2016.

[113] Amy Adele Hasinoff. Sexting in Context: Privacy Norms and Expectations. page 24, 2014.

[114] J Amos Hatch. *Doing qualitative research in education settings*. Suny Press, 2002.

[115] Jordan Hayes, Smirity Kaushik, Charlotte Emily Price, and Yang Wang. Cooperative privacy and security: Learning from people with visual impairments and their allies. In *Fifteenth Symposium on Usable Privacy and Security ({SOUPS} 2019)*, 2019.

[116] Weijia He, Maximilian Golla, Roshni Padhi, Jordan Ofek, Markus Dürmuth, Earlence Fernandes, and Blase Ur. Rethinking access control and authentication for the home internet of things (iot). In *27th USENIX Security Symposium (USENIX Security 18)*, pages 255–272, Baltimore, MD, 2018. USENIX Association.

[117] Debby Herbenick, Jessamyn Bowling, Tsung-Chieh (Jane) Fu, Brian Dodge, Lucia Guerra-Reyes, and Stephanie Sanders. Sexual diversity in the United States: Results from a nationally representative probability sample of adult women and men. *PLOS ONE*, 12(7):e0181198, July 2017.

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

[119] Kashmir Hill and Surya Mattu. The house that spied on me. Gizmodo, https://gizmodo.com/the-house-that-spied-on-me-1822429852, 2018. (Accessed on 08/13/2018).

[120] Patricia Hill Collins. Black Feminist Thought in the Matrix of Domination. In *Black Feminist Thought: Knowledge, Consciousness, and the Politics of Empowerment.*, pages 221–238. Routledge, Florence, 2002.

[121] Lynne Hillier, Kimberly J. Mitchell, and Michele L. Ybarra. 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):225–246, 2012.

[122] Christian Pieter Hoffmann, Christoph Lutz, and Giulia Ranzini. Privacy cynicism: A new approach to the privacy paradox. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 10(4), 2016.

[123] Jason Hong. Toward a Safe and Secure Internet of Things. New America, https://www.newamerica.org/cybersecurity-initiative/policy-papers/toward-a-safe-and-secure-internet-of-things/, 2016. (Accessed on 08/13/2018).

[124] Jason I. Hong and James A. Landay. An architecture for privacy-sensitive ubiquitous computing. In *Proceedings of the 2nd International Conference on Mobile Systems, Applications, and Services*, MobiSys '04, pages 177–189, New York, NY, USA, 2004. ACM.

[125] Max Horkheimer. *Critical theory: Selected essays*, volume 1. A&C Black, 1972.

[126] Roberto Hoyle, Robert Templeman, Steven Armes, Denise Anthony, David Crandall, and Apu Kapadia. Privacy behaviors of lifeloggers using wearable cameras. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, UbiComp '14, pages 571–582, New York, NY, USA, 2014. ACM.

[127] Philips Hue. Light your home smarter. https://www2.meethue.com/en-us, 2018. (Accessed on 08/13/2018).

[128] Hilary Hutchinson, Wendy Mackay, Bo Westerlund, Benjamin B. Bederson, Allison Druin, Catherine Plaisant, Michel Beaudouin-Lafon, Stéphane Conversy, Helen Evans, Heiko Hansen, Nicolas Roussel, and Björn Eiderbäck. Technology probes: Inspiring design for and with families. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '03, pages 17–24, New York, NY, USA, 2003. ACM.

[129] Jevan A Hutson, Jessie G Taft, Solon Barocas, and Karen Levy. Debiasing desire: Addressing bias & discrimination on intimate platforms. *Proceedings of the ACM on Human-Computer Interaction*, 2(CSCW):1–18, 2018.

[130] Iulia Ion, Rob Reeder, and Sunny Consolvo. "... no one can hack my mind": Comparing expert and non-expert security practices. In *Eleventh Symposium On Usable Privacy and Security ({SOUPS} 2015)*, pages 327–346, 2015.

[131] Timo Jakobi, Corinna Ogonowski, Nico Castelli, Gunnar Stevens, and Volker Wulf. The catch(es) with smart home: Experiences of a living lab field study. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, CHI '17, pages 1620–1633, New York, NY, USA, 2017. ACM.

[132] Meg Leta Jones. Privacy without screens & the internet of other people's things. *Idaho Law Review*, 2015.

[133] Clara Rübner Jørgensen, Annalise Weckesser, Jerome Turner, and Alex Wade. Young people's views on sexting education and support needs: Findings and recommendations from a UK-based study. *Sex Education*, 19(1):25–40, 2019.

[134] LeeAnn Kahlor. Prism: A planned risk information seeking model. *Health communication*, 25(4):345–356, 2010.

[135] Joe L. Kincheloe and Peter Mclaren. Rethinking Critical Theory and Qualitative Research. In Kecia Hayes, Shirley R. Steinberg, and Kenneth Tobin, editors, *Key Works in Critical Pedagogy*, pages 285–326. SensePublishers, Rotterdam, 2011.

[136] Kami Kosenko, Geoffrey Luurs, and Andrew R Binder. Sexting and sexual behavior, 2011–2015: A critical review and meta-analysis of a growing literature. *Journal of computer-mediated communication*, 22(3):141–160, 2017.

[137] Natalie A. Koziol and Christopher R. Bilder. MRCV: A package for analyzing categorical variables with multiple response options. *R Journal*, 6(1):144–150, 2014.

[138] Amanda Lenhart, Michele Ybarra, and Myeshia Price-Feeney. Nonconsensual Image Sharing. page 9. https://datasociety.net/output/nonconsensual-image-sharing/.

[139] Ada Lerner, Helen Yuxun He, Anna Kawakami, Silvia Catherine Zeamer, and Roberto Hoyle. Privacy and activism in the transgender community. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pages 1–13, 2020.

[140] Karen Levy and Bruce Schneier. Privacy threats in intimate relationships. *Journal of Cybersecurity*, 6(1), May 2020.

[141] Calvin Liang, Jevan Alexander Hutson, and Os Keyes. Surveillance, stigma & sociotechnical design for HIV. *First Monday*, September 2020.

[142] Julia R. Lippman and Scott W. Campbell. Damned if you do, damned if you don't... if you're a girl: Relational and normative contexts of adolescent sexting in the United States. *Journal of Children and Media*, 8(4):371–386, 2014.

[143] Adam Liptak. Civil rights law protects gay and transgender workers, Supreme Court rules. *The New York Times*, 1, 2020.

[144] Tara Lyons, Andrea Krüsi, Leslie Pierre, Thomas Kerr, Will Small, and Kate Shannon. Negotiating violence in the context of transphobia and criminalization: The experiences of trans sex workers in Vancouver, Canada. *Qualitative health research*, 27(2):182–190, 2017.

[145] Sheri Madigan, Anh Ly, Christina L. Rash, Joris Van Ouytsel, and Jeff R. Temple. Prevalence of Multiple Forms of Sexting Behavior Among Youth: A Systematic Review and Meta-analysis. *JAMA Pediatrics*, 172(4):327–335, 04 2018.

[146] Lindsay Mahowald, Sharita Gruberg, and John Halpin. 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.

[147] Alice Marwick, Claire Fontaine, and Danah Boyd. "Nobody sees it, nobody gets mad": Social media, privacy, and personal responsibility among low-SES youth. *Social Media+ Society*, 3(2):2056305117710455, 2017.

[148] Alice E Marwick and danah boyd. Networked privacy: How teenagers negotiate context in social media. *New Media & Society*, 16(7):1051–1067, November 2014.

[149] Adrienne Matei. The war on (unwanted) dick pics has begun. The Guardian, September 2019. https://www.theguardian.com/lifeandstyle/2019/sep/19/its-a-violation-the-war-on-unwanted-dick-pics-has-begun.

[150] Louise Matsakis. The Motherboard guide to sexting securely. Vice, https://www.vice.com/en$_u$s/article/mb3nd4/how − to − sext − securely − safely − what − apps − to − use − sexting, 2017.

[151] Tara Matthews, Kerwell Liao, Anna Turner, Marianne Berkovich, Robert Reeder, and Sunny Consolvo. "She'll just grab any device that's closer": A study of everyday device & account sharing in households. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, 2016.

[152] Tara Matthews, Kathleen O'Leary, Anna Turner, Manya Sleeper, Jill Palzkill Woelfer, Martin Shelton, Cori Manthorne, Elizabeth F. Churchill, and Sunny Consolvo. Stories from survivors: Privacy & security practices when coping with intimate partner abuse. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, CHI '17, pages 2189–2201, New York, NY, USA, 2017. ACM.

[153] Michelle L. Mazurek, J. P. Arsenault, Joanna Bresee, Nitin Gupta, Iulia Ion, Christina Johns, Daniel Lee, Yuan Liang, Jenny Olsen, Brandon Salmon, Richard Shay, Kami Vaniea, Lujo Bauer, Lorrie Faith Cranor, Gregory R. Ganger, and Michael K. Reiter. Access control for home data sharing: Attitudes, needs and practices. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '10, pages 645–654, New York, NY, USA, 2010. ACM.

[154] Michelle L. Mazurek, Peter F. Klemperer, Richard Shay, Hassan Takabi, Lujo Bauer, and Lorrie Faith Cranor. Exploring reactive access control. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '11, pages 2085–2094, New York, NY, USA, 2011. ACM.

[155] Linda C. McClain. Inviolability and privacy: The castle, the sanctuary, and the body. *7 YALE J.L. & HUMAN. 195, 241*, 1995.

[156] Aleecia M McDonald and Lorrie Faith Cranor. The cost of reading privacy policies. *Isjlp*, 4:543, 2008.

[157] Allison McDonald, Catherine Barwulor, Michelle L Mazurek, Florian Schaub, and Elissa M Redmiles. "It's stressful having all these phones": Investigating Sex Workers' Safety Goals, Risks, and Practices Online. In *30th USENIX Security Symposium (USENIX Security 21)*, 2021.

[158] Nora McDonald and Andrea Forte. The politics of privacy theories: Moving from norms to vulnerabilities. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pages 1–14, 2020.

[159] 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):1–23, 2019.

[160] Susan E. McGregor, Polina Charters, Tobin Holliday, and Franziska Roesner. Investigating the Computer Security Practices and Needs of Journalists. *USENIX Security Symposium*, 2015.

[161] Mary L. McHugh. Interrater reliability: the kappa statistic. *Biochemia Medica*, 22(3), Oct. 2012.

[162] Sarah Mennicken and Elaine M. Huang. Hacking the natural habitat: An in-the-wild study of smart homes, their development, and the people who live in them. In Judy Kay, Paul Lukowicz, Hideyuki Tokuda, Patrick Olivier, and Antonio Krüger, editors, *Pervasive Computing*, pages 143–160, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg.

[163] Sarah Mennicken, Amy Hwang, Rayoung Yang, Jesse Hoey, Alex Mihailidis, and Elaine M. Huang. Smart for life: Designing smart home technologies that evolve with users. In *Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems*, CHI EA '15, pages 2377–2380, New York, NY, USA, 2015. ACM.

[164] Sarah Mennicken, Jo Vermeulen, and Elaine M. Huang. From today's augmented houses to tomorrow's smart homes: New directions for home automation research. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, UbiComp '14, pages 105–115, New York, NY, USA, 2014. ACM.

[165] Maurice Merleau-Ponty. *Phenomenology of perception*. Routledge, 1982.

[166] Danaë Metaxa-Kakavouli, Kelly Wang, James A. Landay, and Jeff Hancock. Gender-inclusive design: Sense of belonging and bias in web interfaces. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, CHI '18, pages 614:1–614:6, New York, NY, USA, 2018. ACM.

[167] Miriam J Metzger, Andrew J Flanagin, and Ryan B Medders. Social and heuristic approaches to credibility evaluation online. *Journal of communication*, 60(3):413–439, 2010.

[168] Robert Meyer and Michel Cukier. Assessing the attack threat due to irc channels. pages 467–472, 02 2006.

[169] Hendrik Müller, Aaron Sedley, and Elizabeth Ferrall-Nunge. Survey research in HCI. In *Ways of Knowing in HCI*. Springer-Verlag New York, New York, NY, USA, 2014.

[170] Nest. Nest thermostats — keep you comfortable and help save energy. https://nest.com/thermostats/, 2018. (Accessed on 08/13/2018).

[171] Frank Newport. In U.S., estimate of LGBT population rises to 4.5%, 2018. https://news.gallup.com/poll/234863/estimate-lgbt-population-rises.aspx.

[172] Helen Nissenbaum. Privacy as contextual integrity. *Wash. L. Rev.*, 79:119, 2004.

[173] Anna North. One state has banned unsolicited dick pics. Will it fix the problem? Vox, September 2019. https://www.vox.com/policy-and-politics/2019/9/3/20847447/unsolicited-dick-pics-texas-law-harassment.

[174] Fayika Farhat Nova, Michael Ann Devito, Pratyasha Saha, Kazi Shohanur Rashid, Shashwata Roy Turzo, Sadia Afrin, and Shion Guha. "facebook promotes more harassment": Social media ecosystem, skill and marginalized hijra identity in bangladesh. *CSCW 2021*, February 2021.

[175] Natalie Oswin and Eric Olund. Governing intimacy. *Environment and Planning D: Society and Space*, 28(1):60–67, 2010.

[176] Antti Oulasvirta, Aurora Pihlajamaa, Jukka Perkiö, Debarshi Ray, Taneli Vähäkangas, Tero Hasu, Niklas Vainio, and Petri Myllymäki. Long-term effects of ubiquitous surveillance in the home. In *Proceedings of the 2012 ACM Conference on Ubiquitous Computing*, UbiComp '12, pages 41–50, New York, NY, USA, 2012. ACM.

[177] Kentrell Owens, Camille Cobb, and Lorrie Cranor. "You Gotta Watch What You Say": Surveillance of Communication with Incarcerated People. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, pages 1–18, 2021.

[178] Leysia Palen and Paul Dourish. Unpacking "privacy" for a networked world. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '03, pages 129–136, New York, NY, USA, 2003. ACM.

[179] Erdman B Palmore. Predictors of the longevity difference: a 25-year follow-up. *The Gerontologist*, 22(6):513–518, 1982.

[180] Cheul Young Park, Cori Faklaris, Siyan Zhao, Alex Sciuto, Laura Dabbish, and Jason Hong. Share and share alike? An exploration of secure behaviors in romantic relationships. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, pages 83–102, Baltimore, MD, August 2018. USENIX Association.

[181] Justin W Patchin and Sameer Hinduja. It is time to teach safe sexting. *Journal of Adolescent Health*, 66(2):140–143, 2020.

[182] James Pierce, Sarah Fox, Nick Merrill, and Richmond Wong. Differential Vulnerabilities and a Diversity of Tactics: What Toolkits Teach Us about Cybersecurity. 2:23.

[183] Anthony T. Pinter, Morgan Klaus Scheuerman, and Jed R. Brubaker. Entering Doors, Evading Traps: Benefits and Risks of Visibility During Transgender Coming Outs. *Proceedings of the ACM on Human-Computer Interaction*, 4:1–27, January 2021.

[184] Erika Shehan Poole, Marshini Chetty, Rebecca E Grinter, and W Keith Edwards. More than meets the eye: Transforming the user experience of home network management. *Proceedings of the 7th ACM conference on Designing interactive systems*, pages 455–464, 2008.

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

[186] Emilee Rader, Rick Wash, and Brandon Brooks. Stories as informal lessons about security. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*, SOUPS '12, New York, NY, USA, 2012. Association for Computing Machinery.

[187] Elissa M Redmiles, Jessica Bodford, and Lindsay Blackwell. "I just want to feel safe": A diary study of safety perceptions on social media. In *Proceedings of the International AAAI Conference on Web and Social Media*, volume 13, pages 405–416, 2019.

[188] Elissa M Redmiles, Sean Kross, and Michelle L Mazurek. How I learned to be secure: a census-representative survey of security advice sources and behavior. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pages 666–677, 2016.

[189] Elissa M Redmiles, Amelia R Malone, and Michelle L Mazurek. I think they're trying to tell me something: Advice sources and selection for digital security. In *2016 IEEE Symposium on Security and Privacy (SP)*, pages 272–288. IEEE, 2016.

[190] Elissa M Redmiles, Noel Warford, Amritha Jayanti, Aravind Koneru, Sean Kross, Miraida Morales, Rock Stevens, and Michelle L Mazurek. A Comprehensive Quality Evaluation of Security and Privacy Advice on the Web. page 21.

[191] Robert W. Reeder, Iulia Ion, and Sunny Consolvo. 152 simple steps to stay safe online: Security advice for non-tech-savvy users. *IEEE Security and Privacy*, 2017.

[192] Jake Reichel, Fleming Peck, Mikako Inaba, Bisrat Moges, Brahmnoor Singh Chawla, and Marshini Chetty. 'I have too much respect for my elders': Understanding South African Mobile Users' Perceptions of Privacy and Current Behaviors on Facebook and WhatsApp. In *29th USENIX Security Symposium (USENIX Security 20)*, pages 1949–1966, 2020.

[193] Jeffrey H Reiman. Privacy, intimacy, and personhood. *Philosophy & Public Affairs*, pages 26–44, 1976.

[194] John K Rempel, John G Holmes, and Mark P Zanna. Trust in close relationships. *Journal of Personality and Social Psychology*, 49(1):95, 1985.

[195] Daniel G. Renfrow and Elisabeth A. Rollo. Sexting on Campus: Minimizing Perceived Risks and Neutralizing Behaviors. *Deviant Behavior*, 35(11):903–920, November 2014.

[196] Juniper Research. Amazon Echo & Google Home to reside in over 50% of U.S. households by 2022, as multi-assistant devices take off. https://www.juniperresearch.com/press/press-releases/amazon-echo-google-home-to-reside, November 2017. (Accessed on 08/13/2018).

[197] Neil Richards and Woodrow Hartzog. Taking trust seriously in privacy law. *Stan. Tech. L. Rev.*, 19:431, 2015.

[198] Rikke Andreassen. Social media surveillance, LGBTQ refugees and asylum. *First Monday*, 26(1), December 2020.

[199] Dorothy E Roberts. *Killing the black body: Race, reproduction, and the meaning of liberty*. Vintage, 1999.

[200] Jennifer A. Rode and Erika Shehan Poole. Putting the gender back in digital housekeeping. In *Proceedings of the 4th Conference on Gender & IT*, GenderIT '18, pages 79–90, New York, NY, USA, 2018. ACM.

[201] Mary Beth Rosson, Hansa Sinha, and Tisha Edor. Design planning in end-user web development: Gender, feature exploration and feelings of success. In *Proceedings - 2010 IEEE Symposium on Visual Languages and Human-Centric Computing, VL/HCC 2010*, pages 141–148, 2010.

[202] Nithya Sambasivan, Amna Batool, Nova Ahmed, Tara Matthews, Kurt Thomas, Laura Sanely Gaytán-Lugo, David Nemer, Elie Bursztein, Elizabeth Churchill, and Sunny Consolvo. "They don't leave us alone anywhere we go": Gender and digital abuse in South Asia. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, CHI '19, New York, NY, USA, 2019. Association for Computing Machinery.

[203] Morgan Klaus Scheuerman, Stacy M. Branham, and Foad Hamidi. Safe Spaces and Safe Places: Unpacking Technology-Mediated Experiences of Safety and Harm with Transgender People. *Proceedings of the ACM on Human-Computer Interaction*, 2:1–27, November 2018.

[204] Morgan Klaus Scheuerman, Jialun Aaron Jiang, Casey Fiesler, and Jed R Brubaker. A framework of severity for harmful content online. *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW2):1–33, 2021.

[205] Morgan Klaus Scheuerman, Katta Spiel, Oliver L. Haimson, Foad Hamidi, and Stacy M. Branham. HCI guidelines for gender equity and inclusivity, 2010. https://www.morgan-klaus.com/sigchi-gender-guidelines.

[206] Alyson Shontell. Actually, snapchat doesn't delete your private pictures and someone found a way to resurface them. Business Insider, 2013. https://www.businessinsider.com/snapchat-doesnt-delete-your-private-pictures-2013-5.

[207] Lucy Simko, Ada Lerner, Samia Ibtasam, Franziska Roesner, and Tadayoshi Kohno. Computer security and privacy for refugees in the United States. In *2018 IEEE Symposium on Security and Privacy (SP)*, pages 409–423. IEEE, 2018.

[208] Scott Skinner-Thompson. Performative privacy. *UCDL Rev.*, 50:1673, 2016.

[209] Scott Skinner-Thompson. Privacy's double standards. *Wash. L. Rev.*, 93:2051, 2018.

[210] Julia Slupska, Scarlet Dawson Dawson Duckworth, Linda Ma, and Gina Neff. Participatory threat modelling: Exploring paths to reconfigure cybersecurity. In *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems*, pages 1–6, 2021.

[211] Samsung SmartThings. Add a little smartness to your things. https://www.smartthings.com/, 2018. (Accessed on 08/13/2018).

[212] Stephen Snow, Frederik Auffenberg, and m. c. schraefel. Log it while it's hot: Designing human interaction with smart thermostats for shared work environments. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, CHI '17, pages 1595–1606, New York, NY, USA, 2017. ACM.

[213] Daniel J Solove. Understanding privacy. 2008.

[214] Emily C. Stasko and Pamela A. Geller. Reframing sexting as a positive relationship behavior. Drexel University, https://www.apa.org/news/press/releases/2015/08/reframing-sexting.pdf, 2015.

[215] J. Sturgess, J. R. C. Nurse, and J. Zhao. A capability-oriented approach to assessing privacy risk in smart home ecosystems. In *Living in the Internet of Things: Cybersecurity of the IoT - 2018*, pages 1–8, March 2018.

[216] Nikki Sullivan. *A critical introduction to queer theory*. NYU Press, 2003.

[217] Paul Taylor. *A survey of LGBT Americans: Attitudes, experiences and values in changing times*. Pew Research Center, 2013.

[218] Samuel Hardman Taylor, Jevan Alexander Hutson, and Tyler Richard Alicea. *Social Consequences of Grindr Use: Extending the Internet-Enhanced Self-Disclosure Hypothesis*, page 6645–6657. Association for Computing Machinery, New York, NY, USA, 2017.

[219] Jeff R. Temple. A primer on teen sexting. *JAACAP Connect*, 2(4):6–8, 2015.

[220] Sabrina Thai and Elizabeth Page-Gould. Experiencesampler: An open-source scaffold for building smartphone apps for experience sampling. In *Psychological Methods*, June 2017.

[221] Kurt Thomas, Devdatta Akhawe, Michael Bailey, Dan Boneh, Elie Bursztein, Sunny Consolvo, Nicola Dell, Zakir Durumeric, Patrick Gage Kelley, Deepak Kumar, Damon McCoy, Sarah Meiklejohn, Thomas Ristenpart, and Gianluca Stringhini. SoK: Hate, Harassment, and the Changing Landscape of Online Abuse. page 21.

[222] D. Townsend, F. Knoefel, and R. Goubran. Privacy versus autonomy: A tradeoff model for smart home monitoring technologies. In *2011 Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, pages 4749–4752, Aug 2011.

[223] Emily Tseng, Diana Freed, Kristen Engel, Thomas Ristenpart, and Nicola Dell. 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*, pages 1–17, 2021.

[224] Emily Tseng, Mehrnaz Sabet, Rosanna Bellini, Harkiran Kaur Sodhi, Thomas Ristenpart, and Nicola Dell. 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.

[225] Blase Ur, Jaeyeon Jung, and Stuart Schechter. The current state of access control for smart devices in homes. In *Workshop on Home Usable Privacy and Security (HUPS)*, July 2013.

[226] Blase Ur, Jaeyeon Jung, and Stuart Schechter. Intruders versus intrusiveness: Teens' and parents' perspectives on home-entryway surveillance. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, UbiComp '14, pages 129–139, New York, NY, USA, 2014. ACM.

[227] Rebecca Venema and Katharina Lobinger. "And somehow it ends up on the internet." Agency, trust and risks in photo-sharing among friends and romantic partners. *First Monday*, 22(7), Jul. 2017.

[228] Jessica Vitak, Kalyani Chadha, Linda Steiner, and Zahra Ashktorab. Identifying women's experiences with and strategies for mitigating negative effects of online harassment. In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*, CSCW '17, page 1231–1245, New York, NY, USA, 2017. Association for Computing Machinery.

[229] Kandrea Wade, Jed R Brubaker, and Casey Fiesler. 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*, pages 1–6, 2021.

[230] Ari Ezra Waldman. Privacy as trust: Sharing personal information in a networked world. *U. Miami L. Rev.*, 69:559, 2014.

[231] Ashley Marie Walker and Michael A DeVito. "'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*, pages 1–15, 2020.

[232] Ashley Marie Walker, Yaxing Yao, Christine Geeng, Roberto Hoyle, and Pamela Wisniewski. Moving beyond'one size fits all' research considerations for working with vulnerable populations. *Interactions*, 26(6):34–39, 2019.

[233] Yang Wang. The third wave? inclusive privacy and security. In *Proceedings of the 2017 New Security Paradigms Workshop*, NSPW 2017, page 122–130, New York, NY, USA, 2017. Association for Computing Machinery.

[234] L. Monique Ward. Understanding the role of entertainment media in the sexual socialization of american youth: A review of empirical research. *Developmental review*, 23(3):347–388, 2003.

[235] Hue Watson, Eyitemi Moju-Igbene, Akanksha Kumari, and Sauvik Das. "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*, pages 1–12, 2020.

[236] Jong-bum Woo and Youn-kyung Lim. User experience in do-it-yourself-style smart homes. In *Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, UbiComp '15, pages 779–790, New York, NY, USA, 2015. ACM.

[237] Allison Woodruff, Sally Augustin, and Brooke Foucault. Sabbath day home automation: "it's like mixing technology and religion". In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '07, pages 527–536, New York, NY, USA, 2007. ACM.

[238] Rayoung Yang and Mark W. Newman. Learning from a learning thermostat: Lessons for intelligent systems for the home. In *Proceedings of the 2013 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, UbiComp '13, pages 93–102, New York, NY, USA, 2013. ACM.

[239] Eric Zeng, Tadayoshi Kohno, and Franziska Roesner. What Makes a "Bad" Ad? User Perceptions of Problematic Online Advertising. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, pages 1–24, 2021.

[240] Eric Zeng, Shrirang Mare, and Franziska Roesner. End user security and privacy concerns with smart homes. In *thirteenth symposium on usable privacy and security ({SOUPS} 2017)*, pages 65–80, 2017.

[241] Serena Zheng, Marshini Chetty, and Nick Feamster. User perceptions of smart home iot privacy. In *ACM Conference on Computer Supported Cooperative Work (CSCW)*, 2018.