Digital (in)security:
safety for queer people of colour in a digitalised world

Lara Okafor

Master's thesis
Informatics: Programming and System Architecture
60 credits

Institute of Informatics
Faculty of Mathematics and Natural Sciences

UNIVERSITY OF OSLO

[June / 2022]

Digital (in)security:

safety for queer people of colour in a digitalised world

Lara Okafor

Master's thesis
Informatics: Programming and System Architecture
Institute of Informatics
Faculty of Mathematics and Natural Sciences
University of Oslo

June 2022

2022

Digital (in)security: safety for queer people of colour in a digitalised world

Lara Okafor

http://www.duo.uio.no/

Trykk: Reprosentralen, Universitetet i Oslo

Abstract

Background: Research about queer people, people of colour, and digital safety has been done separately, but little attention has been paid to the overlap between the three. Using intersectionality as a lens, it follows that queer people of colour are subject to their own context when it comes to digital safety, which makes it a worthwhile research area.

Aim: The aim of this thesis is to explore the experiences of queer people of colour with digital safety.

Methodology: Exploratory qualitative research and design justice.

Methods: Semi-structured interviews and thematic analysis.

Findings: Queer people of colour (QPoC) are vulnerable to attacks on their privacy due to their identity, especially if they are politically active. QPoC are not fully covered by existing privacy regulations, especially trans people, who do not receive extra coverage under GDPR due to gender not being classed as ‘sensitive’. QPoC can experience hacking, harassment, death threats, and rape threats due to their identities online. QPoC have specific security concerns, such as far-right extremists and the potential consequences of tech platforms gathering sensitive data about them. QPoC use a varied set of tactics to try to maintain digital safety, such as restricting content and not using real names on social media profiles, self-censorship, leaving phones behind to prevent location tracking, timed disappearing content, reporting serious incidents to the police, and using coded communication online to alert friends to dangerous situations.

Conclusion: Queer people of colour are targeted online due to their identities, and they often do not have the resources or time to become experts in digital security. Technical systems are rarely designed with them in mind, so they also experience lack of safety due to oversight. Despite this, they use the tools they have at their disposal to stay as safe as possible. This topic deserves further study since this is only initial exploratory research. A possible direct continuation of the research done in this thesis would be setting up a digital security clinic targeted at queer people of colour.

Acknowledgements

A million thanks to the five people who allowed me to interview them for this thesis. This whole thing wouldn't have been possible without you.

Thank you to everyone I'm lucky enough to have as part of my community. Over the years, many of you have asked me: how do we keep ourselves safe? I often ask myself the same. I am hoping that this thesis can be a part of my answer. I want us all to be safe together.

Thank you to Toktam Ramezanifarkhani, Maja van der Velden, and Olaf Owe for being such excellent supervisors on the different parts of this arduous journey.

Thank you to Sushi for sitting with me on Zoom for almost two years and helping me keep track even when my brain was rebelling. You didn't have to do any of it and yet you did.

Thank you to Robin Wall Kimmerer for her wonderful book *Braiding Sweetgrass: Indigenous Wisdom, Scientific Knowledge and the Teachings of Plants*, which I read while I was writing this thesis. It restructured my entire brain and made me rethink scientific research.

And thank you, T, for sitting up with me at strange times and always being ready to talk when I need it.

Contents

1 Introduction

"It's like when we talk about safety online.
It's not just online.
It's safety in a digitalised world."
– interview response

We live in a world that is becoming increasingly connected. With the proliferation of technology, security and privacy are becoming more relevant for everyone, from large corporations to the average individual. According to Taylor & Silver (2019), "it is estimated that more than 5 billion people have mobile devices, and over half of these connections are smartphones" (p. 3). Of course, these 5 billion people are distributed unequally across the world, with factors like age, income level, and country of residence playing a role, but trends point towards a continuing increase in smartphone ownership and internet usage.

In an ideal world, this increased connectivity would only be a positive thing. Digitalisation brings a lot of benefits with it, such as fast and diverse modes of communication, instant access to knowledge, and online purchases. But, as with most things, there is a catch.

While using technology, we leave behind data about ourselves. Something as simple as a personality quiz going around on Facebook can aid in extracting small bits of information that seem innocuous when looked at separately but can be collected to create a larger whole that gives someone a foothold to start an escalating series of attacks (Better Business Bureau, 2020). Important services, such as banking, moving primarily online, means there are an increasing number of ways for our daily lives to be disrupted by online attacks. In some cases, governments may use their control over internet and telephone services to surveil and harass citizens, censor opposing voices, and disrupt unwanted activities. For example, by shutting down phone networks during protests (Human Rights Watch, 2014).

As technology becomes more embedded in our daily routines, it brings with it all of its weaknesses and many of us don't have the capacity to learn to defend against them. Massive corporations and government agencies have ample resources to defend themselves from the diverse set of threats that exist due our dependency on technology, but average individuals, activists, and non-profit organisations usually don't, even though they often face the same threats (Brooks, 2018). Sometimes, they are even specifically targeted because of their identities.

Even though security attacks have become a fairly common occurrence, there is a spectrum of risk which can be affected by facets of our identity. Having specific identities can put a target on people's backs or make the consequences of those attacks more serious than they would otherwise be. For example, many wouldn't think twice if information about their life partner was made public, but it could make a massive difference for someone living in a place where their sexuality is illegal, or so socially unacceptable that it leads to ostracism. These specificities are not well studied.

There is little research in the fields of information security, cybersecurity, or privacy that specifically looks at the experiences of queer people of colour. This thesis will explore the experiences of queer people of colour with digital safety.

1.1 Research questions

To explore the topic of digital safety for queer people of colour, these five research questions have been chosen:

1) Are queer people of colour especially vulnerable to attacks on their privacy?
2) Are queer people of colour fully covered by existing privacy regulations and information security measures?
3) Which specific unsafe situations are queer people of colour exposed to through use of technology?
4) Do queer people of colour have specific security concerns?
5) Which alternative strategies do queer people of colour use to stay safe outside already existing digital security frameworks?

1.2 Motivation

I've spent eight years organising within the LGBTQ+ community. This has included working with several different organisations, organising a grassroots festival, and, most recently, completing a film project about queer black people in Norway. In parallel, I was earning two computer science degrees and working as a software developer. Over time, I noticed that technology was often a double-edged sword for many queer people I knew. The internet is an important place, especially for queer people who are isolated. Most of our community is online, but so is everyone else, including the bigots. The queer community, especially people

of colour, lacks resources, which means most don't have the capacity to prioritise digital security. Because of this, many of the queer people of colour I know do not feel safe online, which jeopardises their access to community.

Community is important for queer people; this is not new. Technology has shifted where we find our community, but it hasn't changed the need. I want to share a true story from the book *Baby, You Are My Religion: Women, Gay Bars, and Theology Before Stonewall* about a lesbian woman stuck in an unhappy marriage with a man. It illustrates how desperate the need for community can be. And why it is so important that queer people have safe access to it, whether it's a gay bar or an online forum. For some queer people today, the internet is that lifeline.

> INFORMANT: Well, I had insomnia. I used to phone up all the gay bars, just to hear them answer the phone … Just to hear the noise, oh yes.
> INTERVIEWER: So you would call and just be on the phone?
> INFORMANT: No, I would just hear the noise and the laughter in the background. I just wanted to be there.
> INTERVIEWER: … it helped you just to know it was out there? (Pause)
> INTERVIEWER: … that's a really special story.
> INFORMANT: Yeah, oh God.
> (Cartier, 2013, p.xii)

> Myrna was married from 1953 to 1968 when she separated, and then divorced her husband in 1970 when no-fault divorce law passed in California. She had terrible insomnia throughout her marriage. "I would get up at one or two a.m. and I would call every gay bar I had the number to from the 1940s. I wouldn't say anything. I would just stay on the phone and listen to the sounds in the background. I would stay on until they hung up, and then I would call another one of my numbers, until I had called all the numbers I had. That was my lifeline." What did it mean to call those bars and to hear the sounds in the background? "That phone. Those numbers. That was my lifeline." she whispered, and put both hands by her heart. "It meant there was a place somewhere—even if I couldn't go there—that place was out there. I could hear it. Freedom." She called the bars two to three times a week like this—for fourteen years.
> (Cartier, 2013, p. 172)

1.3 Terminology

Assigned gender at birth

The gender (usually girl or boy) that is decided at birth. It is usually decided according to visible sex characteristics, such as genitalia.

Biometric identification

Physical characteristics that can be used to uniquely identify a person, such as retina scans, fingerprints, voice, etc.

Cisgender (cis) person

A person whose gender matches the one they were assigned at birth.

Digital safety

The combination of information security, information privacy, and physical, emotional, and mental wellbeing that contribute to an experience of being safe online.

Doxing/Doxxing

The hunt for, and publication without consent, of an individual's private information online.

Genderqueer/Gender nonconforming

Breaking with society's norms around gender.

Grindr

A dating app primarily used by queer people, especially men who have sex with men. Grindr has three membership tiers: Free, XTRA, and Unlimited. The different tiers give access to more functionality as they increase in price, functionality such as disappearing photos and hiding location. Grindr gives free access to certain features that increase security in parts of the world where being queer is criminalised.

Hacker

People who use their skills to exploit weaknesses in technological systems.

Intersectionality

The way discrimination compounds when marginalised identities overlap. For example, a person who experiences racism and queerphobia has a different experience from someone who only experiences racism.

LGBTQ+

Lesbian, Gay, Bisexual, Trans, Queer, and others whose gender/sexuality break with the norms of society. Will sometimes be used interchangeably with queer as an umbrella term.

Marginalisation/marginalised

Browne et al. (2012) use the term 'marginalised' to "refer to the conditions and processes by which particular populations are affected by structural inequities and structural violence in ways that result in a disproportionate burden of ill health and social suffering." (p. 2). 'Structural' refers to the ways inequality is baked into the way the world is organised, on a systemic level. Marginalisation can happen due to sexuality, gender, (dis)ability, class, ethnic or racial background and other categories. The point of using the word is to emphasise that "particular populations are not inherently marginalized, rather, it is the marginalizing conditions that create and sustain inequities." (Browne et al., 2012, p. 2).

Non-binary

Not identifying as a man or a woman.

Queer person

Someone whose gender/sexuality breaks with the norms of society. Will sometimes be used interchangeably with LGBTQ+ as an umbrella term.

Queerphobia

Discrimination against those whose gender/sexuality break with the norms of society.

Person of colour

People who are not white. For example, a black person.

Privacy

Privacy is usually concerned with the handling of personal information; how it is collected, used, stored, and whether the owner of the information is aware and consenting.

Social engineering

Broadly, social engineering is using a series of techniques to manipulate other people into fulfilling an end goal of the social engineer. From an information security perspective, social engineering can be defined as a method of wrongly convincing an authorised person to gain access to their resources (machines, passwords, servers, etc.).

SWAT/SWATing

Sending police to the somebody's home under false pretences, such as reporting an active shooter at the address. In the worst case, this can lead to the victim of the SWATing being shot by law enforcement.

Transgender (trans) person

A person whose gender does not match the one they were assigned at birth.

Trolling

Posting online in ways usually meant to elicit a negative reaction.

Undocumented

People that do not have the legal right to reside in the country they are residing in.

2 Background

This background chapter will summarise some existing literature on information privacy, information security, and diversity in the tech industry.

2.1 Information privacy

2.1.1 What is information privacy?

Privacy is commonly seen as an issue of ethics and human rights. Article 12 of the Universal Declaration of Human Rights (United Nations, 1948) states: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

Privacy has different meanings depending on context. Smith et al. (2011) divide the most common usages into general privacy, physical privacy, and information privacy in their review of existing privacy research. Where physical privacy "concerns *physical* access to an individual and/or the individual's surroundings and private space" and information privacy "concerns access to individually identifiable personal *information*" (Smith et al., 2011, p. 990). General privacy, which is usually conceptualised in terms of ethics, is defined as a sort of umbrella term that encompasses both physical and information privacy.

Even though information privacy is the most relevant term in the context of this thesis (and will usually be what is meant when referring to privacy), physical and general privacy should be kept in mind. Personal information and physical location are not easily separated in the time of "doxing" and "SWATing" (see section 1.3). The line between information and physical privacy becomes blurred in a situation where someone who is being physically stalked because their privacy was breached online.

2.1.2 Privacy threats

When people think about threats to their privacy, they often think about the stereotypical hacker sitting in a hoodie behind a black screen full of green code. The reality is that privacy can be threatened by many different actors, even ones we think of as "good". State actors, and

companies we patronise, are constrained by privacy regulations precisely because they are in positions to threaten privacy and often do. This section will detail some of the actors that threaten privacy (and sometimes information security) and outline some of the effects that this can have.

State actors

Wikileaks and Edward Snowden are both names that have become known the world over for exposing US government secrets. As recently as 2017, Wikileaks publicised documents detailing how the CIA had exploited flaws in existing internet infrastructure to allow for surveillance (Menn, 2017). Edward Snowden, a former NSA contractor, had to flee from the US to Hong Kong to Russia after leaking classified NSA information that exposed the extent of global surveillance (Burrough et al., 2014). People employed by government agencies are paid to find and exploit flaws in the systems that everyday humans use. This is justified by evoking the spectre of compromised national security, but personal privacy is at stake whenever this is done. The erosion of privacy can lead to decreased safety.

A specific example would be the biometric identification system being used by the UN Refugee Agency (UNHCR) to register Rohingya refugees in Bangladesh. Refugees cannot access aid until they are registered in this system, which does not leave them much choice to refuse. UNHCR shares the data with the Bangladeshi government, which Bangladeshi officials “have publicly stated […] will be used to help in sending the Rohingya refugees back to Myanmar.” (Thomas, 2018). Being sent back to Myanmar can mean persecution and death for Rohingya refugees. UNHCR implemented this system to support their work and increase efficiency, but it can have far-reaching consequences for the people registered in their databases.

Another example was the Norwegian Smittestopp app, a contact tracing app introduced to keep track of COVID-19 exposures. It was rated as one of the worst contact tracing apps in the world when it came to privacy (Fjeld, 2020).

Tech companies

In this day and age, information is currency. All of the big tech companies traffic in personal information for profit. Individual privacy cannot be a priority for them while they are

incentivised to collect and use as much personal data as possible. Google and Facebook collect so much information about people that they are able to build fairly accurate profiles of their users for use in marketing and content recommendations. This kind of information can be used maliciously if it falls into the wrong hands.

Butler (2007) gives the example of AOL's (America Online's) 2006 decision to publish anonymised data about people's search queries, which quickly had to be reversed because it was possible to figure out some people's identities from the data set, due to things like searches for own names and context clues. Even when companies are trying to do things that are aligned with the public good, like publishing large data sets for researchers to use, there are always privacy implications.

Kosinski et al. (2013) show how a single data point, such as someone's Facebook Likes, can be used to predict traits fairly accurately, such as sexuality, ethnicity, political views, religious beliefs, substance use, age, gender, and more. This kind of predictive power can also be used for things like targeted pregnancy ads, which can have an unfortunate effect on someone that still receives ads after a miscarriage (Moss, 2019) or when an unmarried woman's pregnancy is revealed to her family in a place where it is culturally unacceptable for her to be pregnant (Kosinski et al., 2013, p. 1).

2.1.3 Privacy threats due to identity

People's privacy concerns are going to be filtered through their specific set of experiences. This can lead to divergence from expected behaviour in their meetings with systems they have to interact with. For example, a healthcare system is supposed to help prevent and treat health issues, but that is contingent on patients being honest about what is happening with them.

Eklöf et al. (2015) detail how this is a potential problem for Somali asylum seekers when translators who are a part of patients' cultural communities are used during healthcare appointments. Patients who would be willing to share information with a healthcare provider alone, suddenly find it harder to be completely honest because of worries of the translator not keeping it secret. They are put in a specific situation that people working within the healthcare system might not predict because (1) they do not want sensitive health related information getting back to their own community and (2) they cannot necessarily choose to avoid having

someone from their own community involved in health care situations since a translator is necessary for access.

This can be extrapolated to start thinking about issues of privacy within other systems, like technological ones. Different subgroups are going to have varying ideas of what privacy is and the systems that these subgroups meet will not always be equipped to handle that, because they are designed by people who don't take their specific needs into account (or even know that those needs exist). This can lead to specific information security and privacy threats that usually aren't thought of.

An example of this has already been covered in the case of the UNHCR's use of biometric identification with Rohingya refugees (Thomas, 2018). This system was put into place with the aim of aiding the ability of a humanitarian organisation to do its work, but there are many possible negative consequences because the people being registered in these systems are especially vulnerable.

The Initiative for Equal Rights (2019) say in their report that LGBTQI+ people in Nigeria have been arrested because of information illegally found on their phones by police officers. Nigeria is a country where same sex marriage, cohabitation, community gatherings and other aspects of being LGBTQI+ are criminalised (Human Rights Watch, 2016). LGBTQI+ people have to be worried about their use of technology and social media in case anything they do can be used against them later.

Marginalised people can also be particularly targeted online by harassment campaigns, which can incorporate things like doxing (see section 1.3), which happened to a journalist who experienced Islamophobic harassment after being doxed (Ansari, 2019). He ended up leaving social media. This affects people's wellbeing and their right to free expression.

There are also examples of the rising use of surveillance software at schools leading to situations where young LGBTQ+ people are outed to their families without their consent due to "software that flags any student writing that uses, among other terms, 'queer' or 'transgender.'" (Caraballo, 2022). Legislation that forces people working at schools to disclose such information to students' families makes that kind of software dangerous to queer students.

2.1.4 Privacy regulations

General Data Protection Regulation (GDPR)

The GDPR became enforceable on May 25th, 2018 and is supposed to regulate the processing of data within Europe. It also applies to entities that serve European customers outside of Europe. It is enforced by Data Protection Authorities (DPAs) located in specific European member states, for example, in Norway this would be Datatilsynet. DPAs have the ability to issue warnings, reprimands, bans on processing, and fines for non-compliance. Under GDPR certain categories of personal information, such as race, ethnicity, or sexual orientation are categorised as 'sensitive' and get special protection. Article 5 of the GDPR (2016) outlines the general principles the regulation is supposed to uphold related to processing personal data. Those principles are: (1) 'lawfulness, fairness and transparency', (2) 'purpose limitation', (3) 'data minimisation', (4) 'accuracy', (5) 'storage limitation', (6) 'integrity and confidentiality', and (7) 'accountability' (art. 5). All in all, it regulates people's rights to their personal data and the ways that data processors need to be accountable for the data they are handling.

California Consumer Privacy Act (CCPA)

The CCPA went into effect January 1st, 2020. It is similar to the GDPR, but limited to residents of the state of California, USA. There are less enforcement possibilities, the maximum fine is much lower than for the GDPR and there are no warnings, reprimands, or bans (SB-1121, 2018). There is also no special consideration for 'sensitive' information, so there is no specific protection for marginalised people as there might be under GDPR.

How do regulations impact on privacy threats?

Since the GDPR became enforceable there have been large-scale effects, such as the Commission nationale de l'informatique et des libertés (CNIL), France's DPA, imposing a 50 million euro penalty on Google (CNIL, 2020). This is, of course, important but there are many privacy violations that cannot be stopped by regulation like the GDPR and CCPA.

Hackers who specifically target people cannot be fined or banned through enforcement of these regulations, because they aren't covered by them. Techniques like social engineering will succeed, regardless of whether it is possible to fine Google and Facebook. Regulation has a big part to play in the wider landscape of privacy protection, but it cannot cover all cases.

Even if sanctions are put in place after a privacy violation by a big company, the privacy of individuals has still been compromised and that can be life or death for someone who has sensitive personal information they must hide.

It is important to have an overview of the privacy landscape, but the question of protecting marginalised people from information security and privacy attacks has to be addressed in additional ways aside from regulation. Especially with the CCPA, you can see that these frameworks are meant to protect the 'general' person and not people who are specifically in danger because of their identities. Hopefully, regulations like the GDPR and CCPA will reduce the amount of data gathered by big tech companies and lessen attack surfaces in that way.

2.2 Information security

2.2.1 What is information security?

The International Organization for Standardization (ISO, 2018) defines information security as "preservation of confidentiality, integrity and availability of information […] In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved."

In an information security context:

- *Confidentiality* means that information is only available to those with authorised access.
- *Integrity* means information is accurate and complete.
- *Availability* means information is accessible to authorised entities when needed.
- *Authenticity* means that an entity is who they say they are.
- *Accountability* means that any actions in a system must be traceable to their source.
- *Non-repudiation* is the ability to prove that an action was taken by a specific entity.
- *Reliability* means a system has consistently correct behaviour.

In less formal terms, information security can be said to be about making sure that accurate information is available only to the correct people at the correct times.

When taking a technical viewpoint there are many tools and strategies that can be used to maintain the different aspects of information security. Things like multi-factor authentication (MFA), password managers, encryption, security training, and legal consequences can all contribute to keeping information safe.

However, these kinds of definitions often do not acknowledge social context. There is usually no mention of marginalisation, and why people might be exposed to attacks more often than others. When information security professionals are talking about threat assessments, they rarely list government affiliated groups as potential threat actors, even though some groups of people (sex workers, immigrants, queer people) are exposed to risk through interaction with groups like the police.

With increasing digitalisation, the amount of information to protect multiplies constantly. There is big money in information security, both to gain (Columbus, 2020) and to lose. There have been multiple international incidents that have slowed entire industries to a standstill, such as the WannaCry and Petya malware attacks in 2017 (Auchard et al., 2017; Whittaker, 2019), which encrypted devices worldwide and tried to extort people into paying for decryption. Petya was an attack that started in the Ukraine and had a ripple effect that reached as far as Denmark and Argentina.

These types of threats exist and are constantly evolving, but they do not stand unchallenged. There are many people working on ways to keep information and systems safe. Tools like multifactor authentication, password managers, and encryption are widely available and assist people in keeping themselves and their information safe online. There are also many different types of security training for all levels of expertise. These are important because the biggest threats to security aren't always technological in nature but often created by human behaviour.

2.2.2 Security threats

Whereas threats to privacy can, in some cases, be "technically" legal when systems are working as they should be, threats to information security usually aren't. Information security breaches can also often simultaneously lead to privacy breaches in systems that contain personal information, so the two are related.

People who try to create information security breaches are usually called hackers. They can be divided up into a few different categories, most commonly referred to as “black hat” (malicious intentions), “white hat” (good intentions, otherwise known as “ethical hackers”), and “grey hat” (mixed intentions).

Hackers can use many techniques, such as social engineering and creating and sending out viruses and DDoS attacks. Hackers are usually trying to gain unauthorised access to systems or information, so they tend to pose a threat to both information security and privacy

There is a wealth of software that can be used to assist in automating the hacking process, such as Maltego (a data mining tool), Fingerprinting Organizations with Collected Archives (FOCA, a tool that finds metadata and hidden information in documents) and Medusa (a login brute-forcing tool). These are tools that gather information, organise it and can make thousands of password attempts in a small fraction of the time it would take a person to do it manually.

In a social media age where people post all kinds of information about themselves it is also easier than ever to find an “in”, because things like passwords or answers to security questions are often easier to guess when more information is known about the person that made them (Better Business Bureau, 2020). The tools already mentioned and the wealth of information available online can also assist hackers when using techniques like social engineering.

2.2.3 Security threats due to identity

Most people experience threats to information security in some way, due to the widespread use of technology. But there are factors that affect the types of threats and how vulnerable people are to them. Chen & Dell (2019) write about security and privacy for human trafficking survivors and those working with them. They define human trafficking as “a crime in which a perpetrator, or “trafficker”, preys on vulnerable individuals through atrocities such as sexual exploitation, forced labor, or the removal of organs” (Chen & Dell, 2019, p. 2). For people working to reduce human trafficking, the threat models for themselves and their clients have to include traffickers who may have physical access to devices and log-in information due to ‘low technology literacy’ of victims, these are often not threats that the ‘average’ person has to think about. In Chen & Dell’s (2019) paper there were also concerns expressed

about law enforcement. Whereas most people might look to the police as a source of support in situations where they feel unsafe, in the context of human trafficking there were worries about corrupt police officers being involved in trafficking themselves. Human trafficking survivors were also at risk of being arrested and charged with crimes if they asked for help, because sex work and immigration issues are often criminalised. These are security concerns that have to do with the specific situation and go beyond more general conversations about privacy as a human right. The consequences when security is compromised in this case are also potentially very dire, ranging the spectrum from continued abuse to imprisonment and deportation.

LGBTQ+ people are also exposed to specific threats connected to their gender and/or sexuality. Being LGBTQ+ is criminalised in many countries, which makes them attractive victims, since there aren't many places to go for help as a person whose existence is illegal. Dating apps are potential sources of danger from both criminals and law enforcement, with queer people being lured to what they think are dates and arriving to find officers or gangs waiting to arrest them and/or extort them (Carroll, 2019; Noack, 2014). Rigot (2022) details in a report the ways that the police in Egypt, Lebanon, and Tunisia use digital evidence to target LGBTQ+ people by making fake profiles on dating apps and using force to gain access to queer people's devices, with trans women and gay men (especially if they are low-income and/or refugees) being particularly targeted (p. 46).

Blond et al. (2014) made an empirical analysis of the targeted threats the World Uyghur Congress, an organisation representing the Uyghur ethnic group, experienced. The Uyghurs are a minority ethnic group in China, who are reportedly being sent to labour camps and sterilised due to their ethnicity (BBC, 2021). Blond et al. (2014) found that the "language and topic of the malicious emails were tailored to the mother tongue and level of specialization of the victims." (p. 543). The organisation was targeted because of who they were representing, and the content of the compromised emails was specifically tailored to them.

While everybody can be vulnerable to security threats, the above examples show that context matters. Criminalisation, citizenship status, and cultural acceptance can have effects on which types of people are made into targets. Knowledge about people's identities can also create openings for exploitation. Information security measures cannot work for everyone if they are designed too generally, because everyone doesn't experience the same risks.

There is literature addressing the security vulnerabilities and needs of specific groups of people, such as human trafficking survivors and/or those who've experience intimate partner violence (Havron et al., 2019; Chen & Dell, 2019). However, there isn't much covering racism, queerphobia, and the intersection of the two.

2.3 Lack of diversity in the tech industry

Reports suggest that the tech industry has a diversity problem (Harrison, 2019). Not only is there an issue with recruiting people with marginalised backgrounds (Tiku, 2019; Tiku, 2021), but many companies have inhospitable work cultures and are struggling to retain them (Brammer, 2017; Scott et al., 2017). This shapes the technology that comes out of the industry, but in the context of this thesis the lack of diversity in the tech industry must have an effect on the ways security and privacy are built into technology. If the primary demographic creating security solutions is white, cisgender, heterosexual, able-bodied, and so on, then that will have significant consequences for which types of problems are overlooked and which solutions are chosen.

For every seemingly insurmountable problem that has taken years to become intractable, there will always have been a chorus of quiet voices that someone with more power decided not to listen to. And if those voices weren't heard it is at least partially because the rooms where decisions were being made were made up of a homogenous set of people. After all, like hires like. Rivera (2012) writes about the fact that cultural fit is highly valued in the hiring process. In a world where the cultural activities we participate in are formed by factors like race and class, hiring for cultural fit can end up being a proxy for those factors. Even when companies outsource their hiring to AI algorithms in an attempt at 'fairness', they will often get more of the same because previous patterns are reinforced (Dastin, 2018).

The array of problem scenarios one is able to imagine is the first step to being able to envision a set of solutions. The demographics of the security niche of the tech industry most likely contribute to important solutions being overseen. For example, it is possible that a company like Slack would have taken more time before adding new functionality like extended direct messaging privileges (Statt, 2021) if they had a marginalised person in the room to tell them it would probably lead to increased harassment. This particular feature was later improved to remove some of the potential harassment pathways, but only after user feedback.

Often, the people that know best are the ones actually experiencing the issues, and the tech industry is not always taking advantage of that lived experience. The composition of the tech industry has a large hand in the gaps found in technology. This isn't a problem that can be solved overnight, but one thing that can be done is to ask those who are affected directly, which is the aim of this thesis.

High-profile examples of another part of the problem, tech companies being inhospitable to their marginalised employees, are Timnit Gebru's (a black woman) and M. Mitchell's (a white woman) firings from Google (Vincent, 2021), after conflict arising around attempts to do their work around AI ethics. B. Pagels-Minor (a black non-binary person) and Terra Field (a white trans woman) exited Netflix (Schiffer, 2021) after backlash around Dave Chappelle's transphobic comedy special being streamed on Netflix' platform. Google and Netflix are some of the biggest tech companies in the world and all of these high-profile cases have in common that the employees that end up leaving or being fired are women, LGBTQ+ and/or black. It is hard to know the details of exactly what happened in these labour disputes, especially since there are conflicting accounts, but there is a signalling effect when these types of stories end up making international news.

The people in the tech industry making security and privacy solutions, and deciding how social media platforms operate, set the standards for the experiences people are going to have using technology. The demographics of the tech industry therefore have a significant impact on the subject of this thesis. It is part of the reason that certain people are more overlooked and therefore more likely to have negative experiences online.

3 Conceptual framework

Ravitch & Riggan (2012) define a conceptual framework as "an argument about why the topic one wishes to study matters and why the means proposed to study it are appropriate and rigorous." (p. xiii).

The topic of this thesis isn't covered in the existing literature, therefore it has been necessary to comb through existing theory to find the pieces that fit – a form of bricolage, using "whatever tools and materials are at hand to complete a project" (Levi-Strauss, 1968, as cited in Maxwell, 2013, p. 42) – and turn them into a conceptual framework. The conceptual framework in this thesis consists of four components: (1) experiential knowledge, how a researcher's own personal experience can be used to inform the research design; (2) intersectionality, a concept first coined by Kimberlé Crenshaw, that helps to understand the nature of living with overlapping marginalised identities; (3) social cybersecurity, as an emerging field of research that centres the human in understating safety and security; and lastly (4) strong objectivity, a concept from Feminist Standpoint Theory, which "argues the importance of starting from the experiences of those who have been traditionally left out of the production of knowledge" (Naples, 2017, p. 1).

3.1 Experiential knowledge

Experiential knowledge is the way that a researcher's personal experience can be used to inform their research. Many research paradigms have sought to erase the researcher from their work or strived for neutrality, but more recent developments in qualitative research paradigms have gone against this. For experiential knowledge to be used successfully, there needs to be "critical subjectivity" (Reason, 1988, as cited in Maxwell, 2013, p. 45), which allows for the researcher to use their own experiences and knowledge without them taking over.

Researcher note

I took my first information security class in the autumn of 2018, during the second year of my bachelor's degree. I learned about a lot of terms, concepts, and abbreviations; like attack vectors, Public Key Infrastructure, and CIA (Confidentiality, Integrity, and Availability). I learned very little about the people we are trying to protect and why some of them may need more protecting than others, other than a section on social engineering, which mostly treated

those who were duped by malicious actors as a problem to be fixed. I went on to take a class called Ethical Hacking in 2019, which I found out mainly focused on learning about technical hacking techniques. The 'ethical' in Ethical Hacking just meant not doing anything illegal.

Spring 2020 was the first time I saw humans being centred, when I took a class called 'Public Interest Cybersecurity: The Citizen Clinic Practicum' at University of California, Berkeley. In the Citizen Clinic, the students were divided into interdisciplinary groups and assigned to public interest organisations that needed cybersecurity assistance. I was in a group that worked together with a reproductive rights organisation that had been targeted by white supremacist groups and religious extremists. This experience made it clear to me how important it is for people who don't have the resources to access expensive security consultations to still be able to keep themselves safe. It also made it clear to me how resourceful people are and how much they can find out by themselves when they don't have any other option. Several of the people I was lucky enough to interact with were self-taught experts due to necessity.

As I was learning how to become a technologist, I was also living a life outside of the academy and work. I have worked for several LGBTQ+ organisations through the years, organised a digital festival for queer people of colour, led a film project about black queer people in Norway, and generally spent a lot of time around other queer people.

I kept noticing things that raised questions and fed their way into the thoughts I was having about the direction I wanted to pursue with technology. The organisations I have worked with are under-resourced and helping incredibly vulnerable people. Isn't it as (or more) important that LGBTQ+ asylum seekers are digitally safe, as some corporate entity that has the resources for yearly penetration tests? I also found that people had an incredible number of questions for me whenever they found out what I studied and worked with and seemed to mostly be trying to do the best with what they had, something that felt in opposition to a lot of the information security literature I'd been taught up to that point, which focused on the 'human as the weakest link'.

I noticed interesting patterns, such as the fact that many of the queer people of colour I added on social media after events didn't use their actual names online and rarely had pictures of themselves, more than I experienced in other spaces. I noticed that people had security practices outside of the usual recommendations of turning on multifactor authentication and

using longer passwords. I also noticed, again and again, that a lot of the security recommendations people are expected to adhere to just aren't practical. What if you have memory problems and you're expected to remember a new password for each account you create? What if you're too old to learn how to use a password manager?

I became concerned with the fact that many of the people I knew, people who were doing important work, were afraid to be vocal because of the ways that technology could be used against them. I know multiple people who have been harassed so badly online that they have had to go to the police and get a panic button in case someone who sent them a digital threat actually carries it out. These types of harassment incidents are exhausting and have an effect not just on the person being targeted, but also all the people like them who are watching and realising that it could happen to them too if they're 'too' loud. I think this is an incredible problem in a society that purports to be democratic. I wanted to see what I could do about it with the tools I had, which were my lived experience as a queer person of colour, who was also a technologist with an interest in security. The only problem was that the intersection of those two things was poorly studied.

I started wondering whether there was a way to research the questions that had come up and the things I'd been noticing. Whether there was a way to do security that respected people as experts on their own experiences and not as a 'weak link' in an otherwise perfect information system. Wondering is what lead me to the research questions explored in this thesis.

3.2 Intersectionality

3.2.1 What is intersectionality?

Black feminist thought has created language and frameworks that help to understand the nature of living with multiple identities. One of the better-known terms that has come out of this work is 'intersectionality', coined by Professor Kimberlé Crenshaw in a 1989 paper about the ways that the combination of sexism and racism can turn discrimination against Black women into more than the sum of its parts. In her words: "Discrimination, like traffic through an intersection, may flow in one direction, and it may flow in another. If an accident happens in an intersection, it can be caused by cars traveling from any number of directions and, sometimes, from all of them." (Crenshaw, 1989, p. 149). In other words, when one can be

discriminated on multiple grounds it is rarely possible to pinpoint one reason. For example, a black woman being discriminated against will rarely be able to say it is *just* racism or *just* sexism. The same way a queer person of colour will rarely be able to say it is *just* racism or *just* queerphobia.

Even though intersectionality is the term that has come into mainstream usage, Professor Crenshaw was not the first or last person to work with the concept of discrimination being affected by multiple identities. There are many others, such as Patricia Hill Collins, the Combahee River Collective, bell hooks, Angela Davis, and Audre Lorde.

See section 1.3 for the definition of intersectionality that will be used in this thesis.

3.2.2 Queer people of colour and online safety

Queer people of colour are those who experience discrimination on the grounds of the intersection between their sexuality/gender and race. This thesis will explore digital safety (see section 1.3) for queer people of colour. Using intersectionality as a lens makes it clear that is not enough to study the effects of being queer or being a person of colour separately

To understand the term 'person of colour', it is necessary to talk about race and racism. Race is a concept that is difficult to pin down, since it isn't a biological fact but a social construction, although that doesn't make it any less real. Race is important in this context because racism is tied to racialisation, and not ethnicity or other euphemisms. It is specific to people who are not perceived as white. Whiteness isn't a stable category and can change depending on location – both temporal and geographical. For example, German and Irish immigrants to the United States in the 1800s were initially not seen as white, but were eventually assimilated into whiteness (Asare, 2022). Person of colour used in the context of this thesis will mean someone who is racialised.

Being a queer person of colour shapes people's experience of the world in a specific way. It affects everything; "the job market, the housing market, introduction programmes [for new migrants], meetings with the healthcare system, education" (Eggebø et al., 2018, p. 141). Many people feel like they don't fit in anywhere, because of discrimination that follows them regardless of whether they are trying to interact with majority groups or minority groups that they belong to. "First, I was harassed and discriminated by my family because I'm gay, second of all, it's also really difficult to stand up as an immigrant and actually make it in

Norwegian society – you have to prove that you're good enough all the time – and, thirdly, I'm also discriminated in the gay community. So, where do I belong then?" (Høibråten, 2018, p. 38).

According to Vogels (2021), 68% of lesbian, gay, and bisexual people have personally experienced online harassment, compared to 39% of straight people. Those statistics do not include trans people. According to an article summing up the results of a study, 42% of a sample of 340 young people with ethnic minority backgrounds had experienced direct discrimination online during the first year they were surveyed, this increased to 55% in the second year and 58% in the third year (Tynes, 2015). It's difficult to find numbers for the places where racism and queerphobia (see section 1.3) meet online, but extrapolating from the separate statistics, it isn't likely to be better.

Research points towards both young LGBT people and young people of colour spending more time online (GLSEN et al., 2013; Rideout et al., 2011). At the same time as technology can be a gateway to otherwise physically inaccessible things, it is also an extension of an already racist and queerphobic society.

Does everyone have the right to be safe when using technology? And if so, how do we get there from a world where lesbian, gay, and bisexual people are proportionally experiencing almost twice as much online harassment as their heterosexual counterparts (Vogels, 2021). That data doesn't even include trans people and others who break with the norms of sexuality and gender who are not lesbian, gay, or bisexual.

Information privacy and security deal with protection of private information and technological systems. Experts in these fields often direct their attention to the 'default' person (white, straight, cisgender, able-bodied, etc.) and this most likely leaves dangerous loopholes to be used against people who don't fit that profile. It is important to map possible oversights in this area and also to find possible solutions.

3.3 Social cybersecurity

Carley (2020) defines social cybersecurity as "focused on humans and how these humans can be compromised, converted, and relegated to the unimportant", in contrast to traditional cybersecurity, which is "focused on machines, and how computers and databases can be

compromised" (p. 367). Carley's paper mostly focuses on misinformation, disinformation, and social networks, which are not the main focus of this thesis, but social cybersecurity is still a growing field touching many different disciplines.

"[S]ocial cybersecurity is focused on humans situated in society and how the digital environment can be manipulated to alter both the community and the narrative." (Carley, 2020, p. 367). Exploring how the digital environment affects queer people of colour's experiences of safety, which is the aim of this thesis, aligns with this focus.

Carley (2019) writes that "influence campaigns appearing to come from state level actors during the elections in Western Europe and the US from 2016 to 2020 were often aimed at minorities. For example, they targeted women, ethnic minorities, and the LGBQT community." (Carley, 2020, p. 366). This is in line with the fundamental hypothesis of this thesis: people with marginalised identities have particular security considerations. This thesis focuses on queer people of colour's human experiences of safety connected to information security, cybersecurity, and privacy, which places it into the field of social cybersecurity.

3.4 Strong objectivity

Harding coined the term strong objectivity in 1995. Strong objectivity is a concept that came out of Feminist Standpoint Theory, which argues "that what we do in our social relations both enables and limits (it does not determine) what we can know" (Harding, 1995, p. 341). In other words, our position in life influences our experiences.

Strong objectivity sees the goal of neutrality as standing in the way of objectivity (Harding, 1995). The "importance of starting from the experiences of those who have been traditionally left out of the production of knowledge" (Naples, 2017, p. 1) is prioritized. They are seen as those in the best position to give an objective account, because they have a "greater motivation […] to understand the views or perspectives of those in positions of power" (Naples, 2017, p. 1).

Queer people of colour have not typically been included in research efforts around technology. This thesis incorporates the concept of strong objectivity by centring queer people of colour as experts on their own experiences.

4 Research approach

4.1 Methodology

This thesis aims to gain insights into the ways that queer people of colour experience, and try to maintain, safety online. The goal in this thesis isn't statistical analysis, but information that allows a deep look into the experiences of people in marginalised groups, which formed the choice of methodology. The next two sections will expand on the methodology of this thesis.

4.1.1 Design Justice

The Design Justice framework strongly influences the methodology of this thesis. There is a focus on community-centred research, respect for lived experience, and reframing what an 'expert' is. This has influenced the choice of methodology, methods, and the aims of the thesis itself. Another approach to doing this research could have been interviewing 'experts' in the field to map the ways they think about, and work for, queer people of colour. But that wouldn't allow for the emphasis on people knowing best about their own experience, which is also in line with strong objectivity (see section 3.4).

This thesis adheres strongly to similar principles as those laid out in Costanza-Chock's Design Justice (2018). Especially principles 2, 4, 5, and 10.

Design Justice principles

1) We use design to sustain, heal, and empower our communities, as well as to seek liberation from exploitative and oppressive systems.

2) **We center the voices of those who are directly impacted by the outcomes of the design process.**

3) We prioritize design's impact on the community over the intentions of the designer.

4) **We view change as emergent from an accountable, accessible, and collaborative process, rather than as a point at the end of a process.**

5) **We see the role of the designer as a facilitator rather than an expert.**

6) We believe that everyone is an expert based on their own lived experience, and that we all have unique and brilliant contributions to bring to a design process.

7) We share design knowledge and tools with our communities.

8) We work towards sustainable, community-led and -controlled outcomes.

9) We work towards non-exploitative solutions that reconnect us to the earth and to each other.

10) **Before seeking new design solutions, we look for what is already working at the community level. We honor and uplift traditional, indigenous, and local knowledge and practices.**

(Costanza-Chock, 2018, p. 1)

The fundamental assumption is not that those being interviewed are inexpert users who need to be rated according to an arbitrary list of security habits decided by 'experts', but that their experiences are illuminating for what professionals need to take notice of and that users are also able to find their own novel solutions within the constraints of the systems they are using. Technology will always have glaring gaps if no conversations are being had with the people who are actually using it, especially those who are most vulnerable. Creating safety for those who are most at risk will often have a positive trickledown effect for the more general user. This thesis aims to be a step in the direction of mapping some of the gaps and also making some suggestions for where to start looking for solutions in a way that centres those most at risk.

4.1.2 Exploratory qualitative research

Yin (2015) characterises qualitative research as:

1. Studying the meaning of people's lives, under real-world conditions;

2. Representing the views and perspectives of the people in a study;

3. Covering the contextual conditions within which people live;

4. Contributing insights into existing or emerging concepts that may help to explain human social behavior; and

5. Striving to use multiple sources of evidence rather than relying on a single source alone (pp. 7-8).

The conceptual framework and the methodological influence of design justice on this thesis made qualitative research the most fitting choice. It would be difficult to recruit enough respondents to make statistically significant conclusions and it wouldn't necessarily be suitable for an early foray into the subject area. The problem area of this thesis is still largely unmapped, and the research questions do not lead to a straightforward testable hypothesis. An exploratory qualitative research methodology was therefore chosen as the most appropriate, since it lends itself well to an in-depth focus on the mostly unexplored first-hand experiences of a relatively small group's (queer people of colour living in Oslo) digital safety. Qualitative research's "emphasis on descriptions rather than numbers" (Maxwell, 2013, p. 30) also allows for an evocative presentation of the lived experiences and knowledge of the informants that wouldn't necessarily be possible with quantitative research.

4.2 Methods

4.2.1 Data collection: semi-structured interviews

Semi-structured interviews were chosen as the data collection format since the desire was to allow respondents more freedom in their responses and give room for an interplay between interviewee and interviewer. Robson (2002) posits that semi-structured interviews are a fitting data collection method when doing exploratory research. Other data collection methods, such as questionnaires or literature review, weren't deemed as appropriate, due to factors such as being too prescriptive and not allowing enough flexibility in the data gathering process or not being suitable to a subject area with little pre-existing literature.

Sandelowski (1995) states that "[a]n adequate sample size in qualitative research is one that permits – by virtue of not being too large – the deep, case-oriented analysis that is a hallmark of all qualitative inquiry, and that results in – by virtue of not being too small – a new and richly textured understanding of experience." (p. 183). Holloway & Galvin (2016) posit most qualitative research samples are comprised of 4-20 informants (p. 151). Data was collected

through five semi-structured interviews. The number of informants was deemed appropriate to gain the depth needed, since the community being researched is not large.

Interviewees were found through convenience sampling. The researcher is already a part of the community in question, so there were existing relationships before the research started which aided the sampling process.

An interview guide was prepared before interviews began. Questions in the interview guide were chosen with help of the conceptual framework and discussion with supervisors. The interview guide was also iterated upon during the interview period, since relevant topics that had not already been in the guide came up during interviews, such as travel. In this way, the interviewees were a part of structuring the interview questions as well. The interview guide ended up including 21 interview questions. The guide is attached (see Appendix A).

Due to COVID-19, two of the interviews were digital. The remaining three were physical. This may have affected interview quality since it is harder to pick up on cues like body language when speaking through a screen. Although some of that effect may have been mitigated due to already existing relationships between interviewer and interviewees which means there was already trust and rapport regardless of format.

Two of the interviews were carried out in Norwegian and three in English. The Norwegian interviews were translated to English during transcription, which means that some meaning could have been lost. Loss of meaning was likely mitigated due to the researcher being fluent in both languages and familiar with the interviewees.

Table 1 *Interview metadata*

Interviewee	Interview length (hh:mm:ss)	Number of transcribed pages	Interview language
1	02:13:54	11	English
2	01:12:30	11	English
3	01:53:49	15	English
4	01:33:22	12	Norwegian
5	00:46:43	6	Norwegian

To preserve anonymity, identifying information will not be tied to specific interview answers, but the general demographics of the interviewees at the time of the interviews were:

- Ages: 23-33
- Ethnic backgrounds (some interviewees used multiple descriptors): Northern Europe, Southwestern Asia, East Asia, North Africa, and West Africa
- Gender/sexuality (some interviewees used multiple descriptors): non-binary, queer, bisexual, woman, fluid, cis man, trans, genderqueer, gender nonconforming

All interviewees were queer and a person of colour.

4.2.2 Data analysis: thematic analysis

Thematic analysis (TA) was chosen as the data analysis method for this thesis. TA was chosen due to it being a fitting analysis method for researchers new to qualitative research with guidance from the clear step-by-step instructions laid out in Braun & Clarke (2006) (see Table 2). TA allows for the discovery of themes that exist in data, as opposed to imposing meaning externally, which can then be used to create a compelling narrative. It is a fitting analysis method for exploratory qualitative research grounded in strong objectivity and design justice because it is not about neutrally pretending to 'give voice' to participants (Braun & Clarke, 2006, p. 80), it is about an interplay between that which resides in the data and the researcher's understanding of the data. As Brown & Clarke stated: "Any theoretical framework carries with it a number of assumptions about the nature of the data, what they represent in terms of the 'the world', 'reality', and so forth. A good thematic analysis will make this transparent." (p. 81). The TA employed in this thesis is more inductive than deductive, which means "the themes identified are strongly linked to the data themselves" (Braun & Clarke, 2006, p. 83).

Table 2 *'Phases of thematic analysis'*

Phase	Description of the process
1. Familiarizing yourself with your data:	Transcribing data (if necessary), reading and re-reading the data, noting down initial ideas.
2. Generating initial codes:	Coding interesting features of the data in a systematic fashion across the entire data set, collating data relevant to each code.
3. Searching for themes:	Collating codes into potential themes, gathering all data relevant to each potential theme.
4. Reviewing themes:	Checking if the themes work in relation to the coded extracts (Level 1) and the entire data set (Level 2), generating a thematic 'map' of the analysis.
5. Defining and naming themes:	Ongoing analysis to refine the specifics of each theme, and the overall story the analysis tells, generating clear definitions and names for each theme.
6. Producing the report:	The final opportunity for analysis. Selection of vivid, compelling extract examples, final analysis of selected extracts, relating back of the analysis to the research question and literature, producing a scholarly report of the analysis.

(Braun & Clarke, 2006, p. 87)

Thematic analysis process

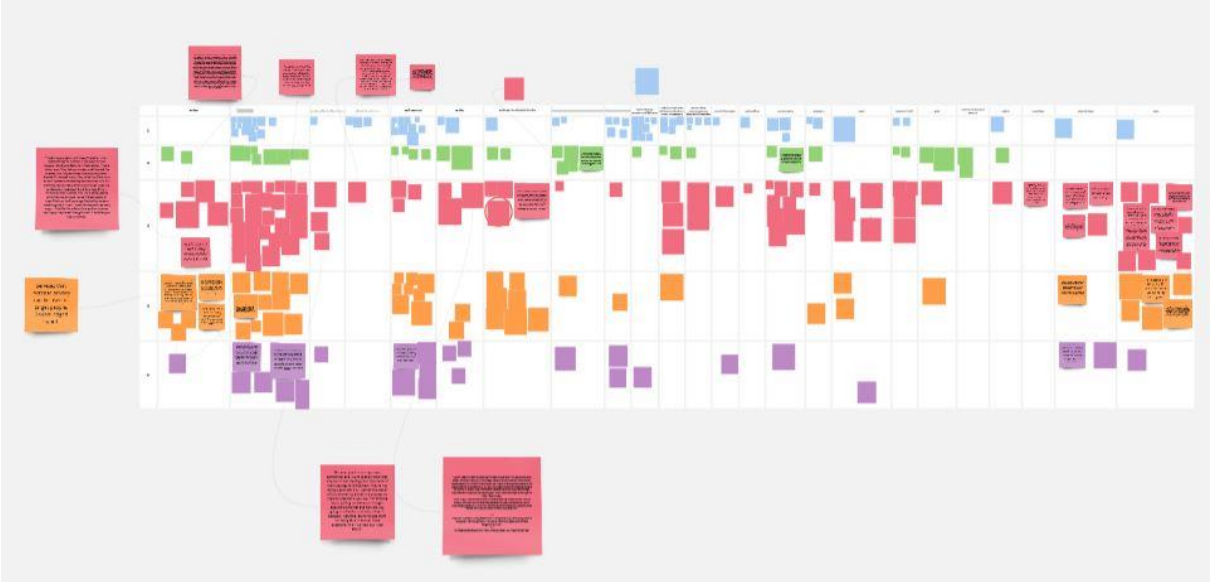
Thematic analysis done on the data for this thesis was done according to the steps seen in Table 2.

Familiarizing yourself with your data: All interviews were fully transcribed and coded by hand. Two of the interviews had to be translated from Norwegian to English while transcribing. Personally handling the interview data increases familiarity with the material and is helpful when going on to code and analyse.

Generating initial codes: Transcribed versions of interviews were printed out and coded by hand.

Searching for themes: Codes were organised into initial themes with the help of a Miro board, see figure below.

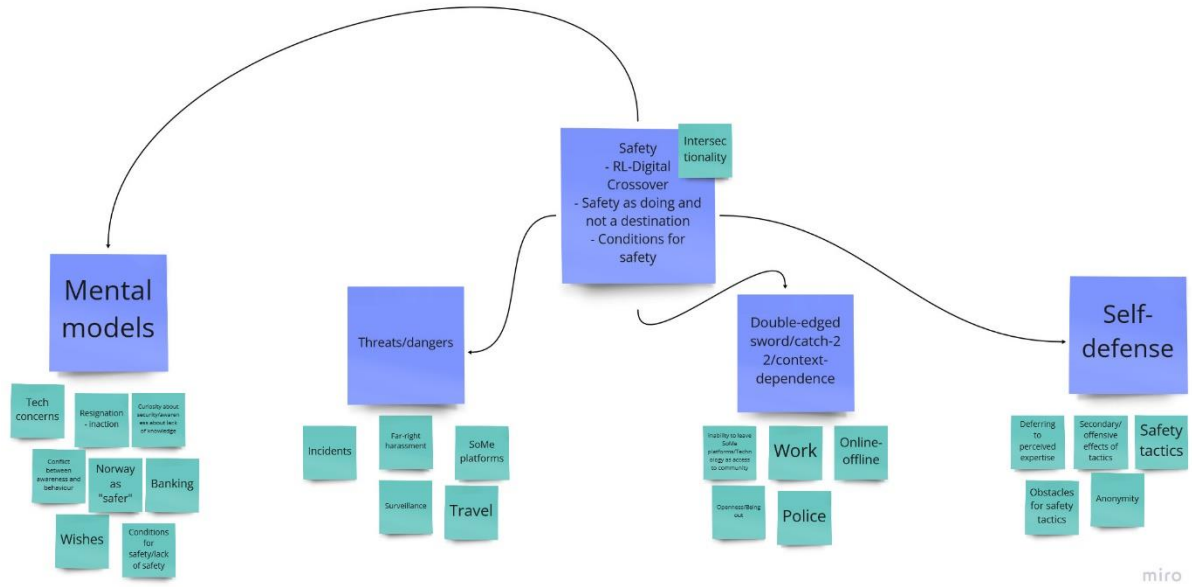
Figure 1 *Codes organised into initial themes*



Above figure is in low resolution to prevent identifying information being visible.

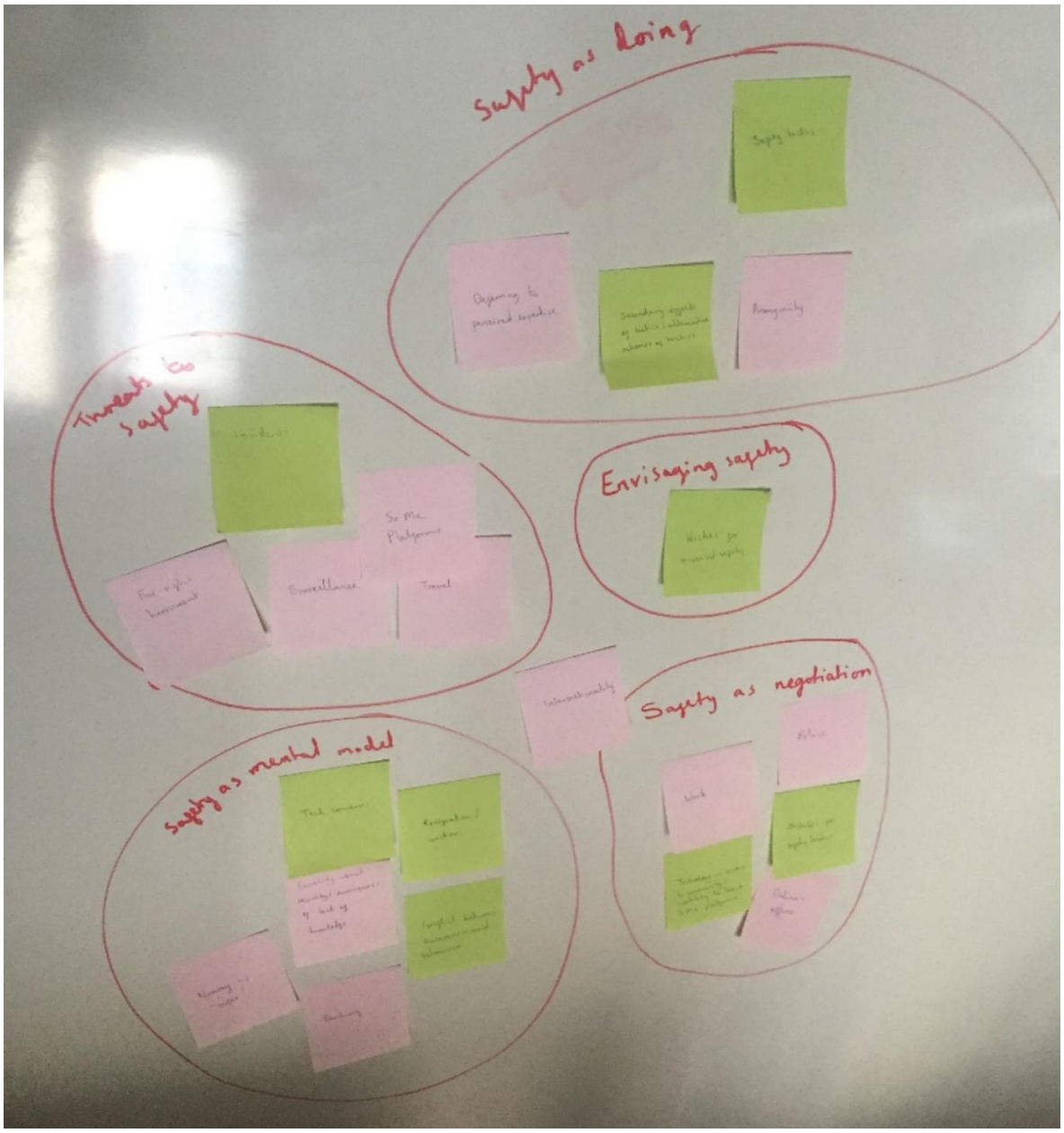
Reviewing themes: The initial themes were organised into a set of overarching themes, see figure below.

Figure 2 *Initial overarching themes*



Defining and naming themes: The themes were then moved onto post-it notes on a physical whiteboard to allow for shuffling around and refining of ideas, see figure below.

Figure 3 *Final themes*



Producing the report: The results of this step of the thematic analysis can be read in chapter 5 and 6.

4.3 Ethical considerations

The Norwegian Centre for Research Data (NSD) processes applications and gives feedback to researchers to let them know if they are complying with data handling requirements. This

includes creating suitable consent forms, making it clear how data will be stored and when it will be deleted, and deciding how data should be stored according to the sensitivity of the information. This thesis got an approval from NSD and has been following the steps set out in the application. That has been one check to assure that this thesis is not causing harm in the way data is being stored and handled.

All interviewees were given a written consent form (see Appendix B) before interviews happened and were also informed of the contents of the consent form verbally before each interview started. They were also informed that any information about them could be seen by them or deleted at any time. These were the steps taken to obtain informed consent from those who were willing to be interviewed.

The decision was made not to attach interview transcripts, even anonymised ones, since there is still the risk of identification as the informants were drawn from a relatively small pool of people. Some of the information shared is sensitive, so it would be ethically questionable to put informants at risk of being recognised. For this same reason, a lot of effort was put into anonymising the data.

Care was also taken with data storage. Steps like keeping interview recordings stored separately from other pieces of thesis data and deleting them immediately the transcripts were completed, creating a key to identify interview participants that was stored separately from transcripts, and anonymising transcripts by removing identifying information such as country and place names, names of people, and specific unique events.

On a general level the group being interviewed is potentially very vulnerable. Sharing info from queer people in the closet can be used against them. Norway is a place where it isn't criminalised to be queer. Doing this kind of research in other places would bring a different set of considerations with it.

Another ethical aspect is the positionality of the researcher. The researcher is a member of the group being researched and because it is a relatively small group, the participants were recruited from the researcher's own networks. This raises some potential ethical considerations for the impartiality of the research, but the hope is that it brought with it more benefits than downsides. Since there were already existing relationships previous to the interview, it is probable that it allowed for interviewees to answer questions more candidly

than they might have done otherwise since there would have been an increased level of comfort. It is possible that speaking to someone they knew had the opposite effect, preventing them from sharing things they thought of as embarrassing with someone they knew they would see again, but the answers gained in the interview phase were satisfactory enough that it is unlikely this was the effect.

Impartiality or objectivity is also a difficult thing to gauge. Every researcher brings their own perspective into their research, whether they are affected by the topic or not. The most important part is to be aware how one's positionality is part of the research proceedings. Being an 'outsider' or 'insider' to the research is only a question of point of view.

5 Results

5.1 Theme overview

The thematic analysis process resulted in the main theme of safety, with the subthemes mental models of safety (interviewees thoughts around digital safety), threats to safety (situations that made interviewees feel unsafe online), safety as doing (concrete strategies to keep safe online), negotiating safety (the cost-benefit analyses of staying safe online), and envisaging safety (wishes and visions of a safer future online). Intersectionality was chosen as an underlying theme since it came up in different ways throughout the interviews and is a necessary backdrop to understand the interviewees' experiences. The rest of this chapter will expand on the chosen themes and end with a summary of the results.

Some quotes are altered. Words, phrases, or ellipses in square brackets are there to increase clarity or protect privacy. All gendered pronouns (he/him/his/she/her/hers) have been changed to 'they', 'them', or 'theirs'.

5.2 Intersectionality

The theme of intersectionality formed a foundation for the way interviewees thought about their safety.

Intersectional activism (for example, activism with overlap between queer issues and immigration) was seen as something that increased risk by one interviewee, "The more intersectional activism, the more enemies you have. I would say a white queer person, who's mostly doing local things […] in a Norwegian context. I think it's safer.".

Just existing in Norway as a queer person was also seen as becoming increasingly dangerous the more overlapping marginalised identities one had, "Being queer in Norway, of course it can be dangerous, but when you add geopolitics and asylum and all of these things, when people are undocumented. If these things are added, it's not safe at all."

An interviewee also pointed out that multiple overlapping marginalised identities made research about queer people more sensitive, especially if trying to maintain anonymity, "If

you're part of the queer community or know queer people, it's very easy to know who's who with the right identity markers.".

Interviewees also explicitly compared certain identity markers and saw the overlap of marginalised identities as a source for more fear or sensitivity around certain issues.

> "If I was a heterosexual white man, I don't think I'd be as afraid. To be honest."

> "It is very sensitive for a Black trans person's [explicit] images to get leaked. More than a white cis man, for sure."

Interviewees clearly saw the overlap of marginalised identities as an important factor when it came to the risk different people are exposed to. These viewpoints are important to keep in mind as a backdrop when exploring the overarching theme of 'safety'.

5.3 Safety

After the thematic analysis process was complete, safety was chosen as the main overarching theme, with mental models of safety, threats to safety, safety as doing, negotiating safety, and envisaging safety as subthemes. Intersectionality is a background theme that is interwoven into many of the interviewees' responses. The subthemes are described in more detail in section 5.3.1-5.3.5.

Throughout the interview process it was clear that safety was a complex subject for each interviewee. Since this thesis focuses on exploring the experiences and viewpoints of queer people of colour, there was an effort put towards allowing interviewees to answer as openly as they could, without prescribing too many definitions for them. This meant that safety was conceptualised in many different ways, as exemplified in the following exchange.

> *Interviewer: Do you feel safe when using technology?*

> Interviewee: Define the word safe. Safe physically? Materially? Or...

> *Interviewer: Whatever is relevant.*

> Interviewee: My fear with digital media has different levels.

When talking about digital safety it would be possible to focus on many different aspects. From an information security perspective, for example, it would make sense to ask about concepts like confidentiality, integrity, and availability (see section 2.2.1) or ask in-depth questions about technology usage. However, since this is exploratory qualitative research with a focus on the communities affected (see section 3.4 on strong objectivity and section 4.1.1 on design justice), it was appropriate to focus on the interviewees' experiences without forcing them to deal with sterile technical vocabulary.

Safety therefore ends up meaning many different things in the interviewees' responses, but the answers are still illuminating and give a first-hand perspective of queer people of colour's experiences online, such as the following.

> *Interviewer: Do you generally feel safe when using technology?*
>
> Interviewee: No. Never. I think about this every fucking day. Every second. Every time I post something.
>
> *Interviewer: So, it's actually a big source of stress?*
>
> Interviewee: Yeah. I would say it's one of the biggest. Me as an activist, me as [ethnicity], me as queer.

Technology is a central part of 21st century life and the following sections will expand on how the queer people of colour interviewed for this thesis think about digital safety.

5.3.1 Mental models of safety

The theme 'mental models of safety' was chosen since each interviewee had their own way of thinking about safety and what it meant to them. It is important to build a picture of how queer people of colour conceive safety to fully explore the overarching theme of 'safety' in the context of this thesis.

When asked what sorts of things concerned them about using technology, interviewees brought up privacy and surveillance related topics, information security concerns (such as viruses), harassment, and insecurities around being able to keep themselves safe online. It also became clear that safety is hard to only narrow down to online experiences since it can have offline consequences.

Interviewees had standard information security concerns, such as viruses and spam e-mail. Interviewees also expressed concern about the ways that technology platforms used their information, such as the following responses.

> "I think my biggest concern would be related to how my information is being kept, especially by big companies like Google and Apple and all those that I use for my phone usually."

> "I don't trust that my information isn't being misused by big tech companies. I think that Apple, Google, Facebook, have a lot of information and I think they let us think that we have control of our own data, but I'm a bit sceptical about that."

Interviewees who were more visible online and had experienced more online harassment seemed to additionally have concerns other than the way big technology platforms handle personal data. For example, one interviewee juxtaposed social media companies with less regulated extremist websites when asked whether they have concerns about how social media platforms use their information, "I do think about it, but I have more trust in their platforms than radical fascist platforms that I also visit.".

One interviewee directly connected their safety to their visibility as an activist and the type of activism they participated in, "The more out and about I am as an activist, the more enemies I have. And the more intersectional activism, the more enemies you have."

Multiple interviewees had insecurities around securing their own digital safety. One interviewee recounted when they had custody of sensitive government documents and how stressful trying to send it to the desired recipients was, "I downloaded […] a couple of files, and I just wanted to try to send it, just to see, but when I sent it, I panicked. I was like 'maybe I sent it wrong, maybe I did it wrong, my whole life will be destroyed'."

Online harassment was a topic that came up consistently, even when the participants hadn't experienced it themselves, they had often seen it happen to people they knew, "You see [acquaintance], he gets [harassment] everywhere, not just online. [Friend] just changed number, because she was harassed, she got some threats."

Concerns related to technology were often related to other issues or had possible repercussions in the physical world. For example, one of the interviewees expressed fears

around the use of dating apps, “And if I get a picture and we agree to meet, what if this person is [dangerous]? It’s these types of fears I have.” Technology was both a tool for gaining community and a potential threat vector. This double-bind, technology and social media being a source of community and danger simultaneously, is something that will be explored more in the section about negotiating safety (see section 5.3.4).

When asked whether they knew what to do if they experienced a breach of privacy or security, one of the interviewees answered: “I have no clue and I should probably get into it, that’s like a basic knowledge.” They also expressed an ambivalence towards a breach: “Then again, I’m poor. What are you going to do with my money? I don’t have any.” Another interviewee also expressed ambivalence, but towards the idea of tech platforms using their information: “Everyone knows [social media platforms] have private information about you. Everyone knows this and has kind of accepted it. In a way, that makes me, maybe, careless?”. The interviewee called themself ‘careless’ but an additional factor is the complex risk assessment they have to do online considering the resources and knowledge they have at their disposal. Interviewees expressed conflicts between their awareness and their behaviour, but also often expressed a desire to learn, and sometimes a frustration over lack of information.

An example that points towards ‘carelessness’ perhaps not being the only experiences is that multiple interviewees brought up banking routines without being asked explicitly about them, which suggests that people make safer choices when they are given the tools to make them.

> “But I know what to do if my cards get stolen. Cancel my cards. Oh, […] one year I was called by the card company, and they were like “hey, somebody has tried to use your card in this and this place” where I hadn’t tried, so then I needed to cancel my card.”

> “Because it’s more difficult for a normal hacker to do stuff. Even though it’s more of a hassle. But I like that, I feel safer with things connected to [Bank ID]. And if anything happens it’s their responsibility. There’s someone who’s responsible.”

A part of interviewees’ risk assessments also seemed to include seeing Norway as relatively ‘safer’ than other countries. For example, one of the interviewees compared their own risk from surveillance to their partner’s risk: “If somebody is surveilling our conversations, that would be worse for [partner], because they’re actually in the US.” When asked if being queer person of colour affected the way they used technology, part of one interviewee’s answer was:

“I think maybe if I lived in a country where I could be persecuted or something it could be something I’ve thought even more about.”. Another interviewee had a more complex view of safety in Norway: “I would say a white queer person, who’s mostly doing local things, even though it’s radical, it’s mostly just in a Norwegian context. I think it’s safer. You can be a hardcore trans activist and, if you’re white and Norwegian, still be quite safe.” According to this interviewee, safety in Norway was dependent on identity and what kind of activism one was doing.

Some interviewees had specific factors that made them feel safer online: “I like to know who I share things with. I prefer if I’ve met them personally. When I know they’re QTIBIPoC [Queer, Trans, Intersex, Black, Indigenous, People of Colour] I’m less wary or if I know I have friends in common.” Social proximity and shared identity markers helped to make one interviewee feel more comfortable adding people on social media. Social proximity wasn’t always a cause for safety though, multiple interviewees talked about differing levels of comfort according to which type of social sphere was present on platforms they used. Facebook was often cited as a place where interviewees felt less comfortable expressing themselves because they had too many conflicting social groups as an audience, including their family. They had to do complex evaluations when deciding what to post where.

> “When it comes to social media, I feel like I always have to check with myself: is this something I really need to post? Who will see it? How will it be interpreted? Is it worth it or not? Is it okay if I don’t share it? Especially when it comes to LGBTQIA+ related issues, but also in recent times, even political stuff.”

One of the interviewees talked about how the internet has affected their sex life:

> “Apps have, digital media has, made sex more unsafe. Unsafe and very accessible. Before the apps you had to go out to have a one night stand, meet people, talk. And there’s always someone who knows someone who knows if that person is crazy or not. But now you don’t know who you’ll end up with.”

Meeting people through the internet removes the ability to vet them through mutual social connections to a certain extent, which is a bigger issue for queer people since their chances of meeting a sexual partner are lower in physical spaces due to stigma and smaller numbers. Even though apps were seen as making the interviewee’s sex life more unsafe due to lack of vetting, the same interviewee recounted that anonymity was important for them before they

were open about their sexuality. When they were asked whether they'd ever been worried about their information being spread online they responded with a yes and elaborated: "Especially when I was in the closet. Because how do you protect yourself? They need to know things, they need to see pictures, that makes it hard to share those sorts of things."

An interviewee expressed that there is a fine line between what is seen as direct hate speech and actions that have an uncomfortable undertone. When asked to define the difference between "uncomfortable messages" and "hate" after recounting unsafe experiences they'd had online, an interviewee stated: "In my case, there wasn't any use of derogatory terms or something that necessarily specifically referenced my identity […] it could be an undertone, or it could be interpreted as something that could be based on stereotypes or assumptions based on my identity." The experience of safety online is often not just about outright hate speech or harassment, but also receiving communication that has undertones of discrimination, which can be harder to identify concretely.

Direct hate speech and harassment did have lasting impacts though. Multiple interviewees had incidents involving online harassment. These left their marks and affected people's inner sense of safety. When asked how receiving threats had affected them, an interviewee responded:

> "I get anxious. I become more aware. I always look over my shoulders and get jumpier. Because these types of incidents, they pass, but they make their mark on you. It's like a little wound. It heals and you don't feel the pain, but you're left with the small scar. It's there, you can always see it. I can still see the scar from when I was six years old and cut myself while chopping onions. This is when I was six, it's still there. People don't see it unless I point it out, but it's still there. Being attacked on digital platforms does the same. Most of them are trolls behind fake profiles, so you don't know what they're capable of. The police say they're mostly just talk, but you don't know. You don't know. You don't know. It could be that you meet ten who are just talk, but the eleventh will act."

Safety online has many dimensions and for many interviewees there were emotional and self-esteem aspects to it: "Safety isn't only about feeling safe from being physically hurt. It's also feeling safe that you're good enough." Feeling unsafe online was emotionally disruptive, in addition to other consequences.

Even interviewees who hadn't experienced any online harassment were wary of far-right extremists online. When asked how they thought they could be made unsafe online, specifically as queer people of colour, two interviewees directly referenced far-right extremists. The first interviewee saying they thought an issue could be "being targeted by all kinds of people, like Nazis and all of those people who tend to hate QTIBIPoC" and the second saying "the only thing I've thought about is organised neo-Nazi groups, 'Den nordiske motstandsbevegelsen' and things like that. Groups that are actively against queer people and don't want to have anything to do with non-white people. Then I can feel a bit unsafe. They can suddenly decide to go after someone who's non-white." Both of these interviewees hadn't had any direct experiences of harassment online and had still considered the topic enough for one of them to name a specific group they were concerned by.

Some interviewees worked at queer organisations and were involved in trying to create safety for other queer people of colour online. One person outlined the ways they did that:

> "We define [my organisation]'s profiles as safe spaces. And we do our best so that people can comment, press like, and participate in relevant discussions. That means we have the responsibility of moderating our feeds so that they are experienced as safe spaces. And always, when we answer or respond to messages or when crises happen, then we move the conversation from digital platforms to face-to-face. Because that's actually the safest way to interact with others, you don't leave digital footprints behind."

First, they had actively thought about how to create safety, part of which they solved with active moderation. The internet platforms that this person's organisation has accounts on are clearly not fulfilling the safety needs of the organisation, since they find it necessary to moderate in addition to what platforms are already doing. The safest option also seemed to be seen as taking things offline. The internet was used as a bridge to get into contact with people but wasn't seen as safe for critical interactions.

The use of the word "safe space" came up in different ways in different interviews. The default state of most internet platforms did not seem to be experienced as safe. Interviewees therefore talked about actively trying to create safe spaces and also expressed wishes for safer spaces.

Safety was often dependent on a lot of factors for interviewees and one quote sums up the issue of digital safety quite succinctly: “It’s like when we talk about safety online. It’s not just online. It’s safety in a digitalised world.”. The things that happen online are often conceptualised as being a separate sphere from other parts of life, but this answer illustrates the fact that being online (especially in a highly digitalised country like Norway) is impossible to divide from offline life.

5.3.2 Threats to safety

Another subtheme that surfaced during the thematic analysis process was titled as ‘threats to safety’. Interviewees were asked about situations that made them feel unsafe online and answered in a variety of ways. From fairly average spam e-mail experiences to hacking attempts from malicious actors.

A clear split in the types of incidents people had experienced online seemed to be related to how politically active they were. This was something interviewees on both sides of the spectrum seemed to be aware of.

> “I’m also not that political on the internet, so I’m not afraid that that can be used against me.”

> “[My digital safety is not affected] because I’m queer and I’m brown. It’s because I’m doing queer, brown activism. […] And that adds extra drama on the internet, more than if I had just been a non-political queer person of colour, who maybe put a post, like ‘Happy Pride’, you know.”

Interviewees recounted a range of incidents when talking about times they had felt unsafe online. Some of those incidents are unlikely to have been connected to their identity in any way, such as having spam e-mails sent from their account and unexpected logins on social media accounts.

Not every ‘average’ experience was so easy to categorise as harmless though. One interviewee got a notification that someone had attempted to login to an account they had on a streaming service. This would have likely gone unremarked if it hadn’t been for the fact that the location of the attempted login was a country that is directly adversarial to this person’s ethnicity. They had already experienced harassment from people from this country. Therefore,

it wasn't as simple as just assuming that it was a run-of-the-mill login attempt from a random hacker. The interviewee described the stress of not knowing whether it was a targeted attempt or not:

> "It could have just been a random scam, it could. […] But because it comes from [Adversarial Country], I'm a bit sceptical. […] I can't trust things being random scams because I have gotten things directly to me too. So, you don't see the normal hacking attempts contra it being because of me being a political being. I don't know the difference sometimes and that adds to the stress. So, I just have to assume the worst because it's safer for me."

For people that have already been made to feel unsafe online, incidents that can't be strictly categorised as targeted can't necessarily be written off. In this specific incident, the previous harassment is tied directly to ethnicity, so the lack of safety is because of who the person is.

Multiple interviewees detailed harassment they had experienced online, ranging from "uncomfortable messages" to death threats. The circumstances of harassment varied. Two interviewees experienced repercussions in the aftermath of publicly expressing themselves:

> "Because of an article I wrote, which I shared on social media [...] me, a politician, and a friend of mine got hacked."

> "When I came out publicly […], I was sent threats via email. I was sent death threats from email addresses that only worked for 24 hours."

A concrete example given by an interviewee of the types of messages they received was this one:

> "One of the death threats I got was from a Facebook profile. That profile is still there. In this message I got a rape threat: 'I will find you. I will fuck you. I will fuck your father, your mother, and your sister.'"

The previous incident was never resolved.

> "The police closed the case because they couldn't find out who was behind that profile. And who's facilitated this? Facebook. Because FB doesn't give out this information. Nothing helped. Nothing. And when the police close these types of

> serious cases, then you become really careful. And it affects your life. And it changes how you behave in your daily life."

Another interviewee described the effects of getting threats over the phone:

> "After that I'm really scared of sharing my phone number with people. Even though a phone number is more difficult to hack than an e-mail or those kinds of things, it hurts more when I hear a voice telling me I'm a whore, I shall be raped if I do this again. It works. They know it works, that's why they're doing it."

One of the interviewees was personally harassed due to their work helping a queer youth:

> "I was working in another queer organisation. I'd sent an email to a […] teen and I had to help them to a crisis centre and the brother easily hacked their sibling's email, […] and they found out that I was helping, and they came to my door. I had to move, I had to change name."

This is a clear example of the way that information found online can have concrete consequences offline. The online-offline divide (or lack of divide) is something multiple interviewees mentioned. Digital safety cannot be separated from physical safety.

> "Harassment online can cross over into real life if they find your personal information."

> "[B]ecause for safety, in real life, you need to have control of safety online."

One interviewee talked about how online harassment is more accessible. The anonymous nature of the internet lowers the threshold for engaging in harassment, which exposes more people to harassment than would happen otherwise.

> "It's so much easier to get high [numbers of harassers] if it's on the internet, because the bullies also feel safer doing it online rather than on the street. The amount of hate is bigger online. It's more dangerous online, it can destroy you and exhaust you much more than something else."

All of the persons interviewed were adults, but some had experiences from when they were younger and not out to their families. When asked whether there were ways that being a queer person of colour affected the way they used technology, an interviewee answered: "Not today,

but when I was still in the closet it was a bigger concern. Especially when I lived at home with my parents. Mostly [it was about] my parents not finding stuff. Things like that, things like erasing my traces."

Interviewees also reflected around the ways that they might have needed to navigate if they had been young in the age of smart phones and social media. For example, "If I'd grown up today, I probably would have had more anonymous social media accounts." Multiple interviewees acknowledged that they would have had to navigate their youth differently if they had been young now.

Interviewees still had experiences with technology in their younger years. Another example was a man with the same ethnicity as an interviewee finding information about them online and then using that information to contact their parents:

> "He found me, I forgot to block him before because I wasn't thinking about him. And he was threatening my parents like 'aha, you have a [child] that's doing this and this and that' and freaked out my parents for nothing."

There was also an interviewee whose romantic interest called them while still living at home with their family:

> "My phone rang, and my [sibling] picked up the phone. And the [romantic interest] on the other end thought it was me. And my [sibling] pretended [they were] me."

Family members having access to the same technology was also an issue:

> "One time I was watching porn and I forgot to exit the page. Then my mother and sister came and wanted to use my laptop. And the first thing when they press the space bar: hardcore gay sex."

One interviewee recounted an incident from a few years ago, involving the Norwegian mobile payment app Vipps.

> "I had a stalker [...] They had my number, and I blocked the number, fine. They called me from another phone, I blocked it. [...] there were at least 8 phone numbers they contacted me with. But then they found a really smart way through Vipps."

At the time, there was no way of blocking people through Vipps, although that feature was introduced eventually after multiple people ran into the same problem (Westeng, 2018). This is an example of how important it is to consider the malicious ways people will use technology while designing it. Slack's attempt to introduce a new direct messaging feature (Statt, 2021) had a similar issue (see section 2.3). Use cases like these are particularly relevant for queer people of colour because research points towards them experiencing as much, if not more, intimate partner violence as the general population (Brown & Herman, 2015).

Social media platforms, their handling of personal information, and potential for exploitation were also topics that came up. One of the interviewees mentioned the fact that they behaved differently and felt varying levels of comfort on different platforms. This seemed to be related to functionality, but also a desire to have control over which people were able to see posts. Facebook and Instagram were the main platforms they mentioned in this sense: "Facebook, I don't really have control over anymore because I started using it so early. With Instagram, that's the platform that I use, where I have followers and post things, I like to know who sees my stuff." Part of the reason they didn't want to post on Facebook was directly related to their gender: "I never know how they will gender me if they comment, so I just don't bother." This can be partially explained by the concept of context collapse (Loh & Walsh, 2021), the merging of usually separate social contexts that often happens on social media. There are few situations in the physical world where a person would have their parents, childhood friends, work colleagues, and internet strangers all in the same place; but this is often the case on social media – especially when people have been on a platform for a long time. Context collapse can be particularly difficult for queer people because not everyone they've added on Facebook since 2008 might have updated information about their gender or sexuality, which can lead to incorrect assumptions when interacting with them online. For the interviewee in this example, it has led to them deciding to not engage at all when they don't feel like they are able to control their social context. The risk of being addressed incorrectly is not worth engaging.

Social media platforms, and technology companies in general, were themselves a source of distrust for interviewees.

> "I don't trust that my information isn't being misused by big tech companies. I think that Apple, Google, Facebook, have a lot of information and I think they let us think that we have control of our own data, but I'm a bit sceptical about that."

Scepticism towards tech platforms' ability to ensure that user privacy isn't breached isn't unusual, but there are extra stakes for people with marginalised identities. One of the interviewees reflected around whether they would be as worried if they weren't queer or a person of colour and concluded that they likely wouldn't be.

> "If a big company had suddenly leaked information to people that have bad intentions, then it would be scary to think I didn't have control over my own data. I think the foundation is the fear that something bad will happen to me or to those around me because information about me has been spread to places it isn't supposed to be. [...] If I was a heterosexual white man, I don't think I'd be as afraid. To be honest."

However, some interviewees seemed to see social media platforms and their data handling as a bad option in a set of worse options, even if they acknowledged that it was an issue. When asked whether they have concerns about big social media platforms, this was one interviewee's response:

> "I do think about it, but I have more trust in their platforms than radical fascist platforms that I also visit. Everyone knows that they have private information about you. Everyone knows this and has kind of accepted it. In a way, that makes me, maybe, careless? But I should [be concerned] because Facebook literally has listened to what [Adversarial Country] has to say and they have come with demands. And Facebook is different in [Adversarial Country]. It's the same platform, the same owners, but different censorship depending on where in the world you are, for example."

They trusted the big social media platforms more than explicitly "radical fascist" platforms, but once they gave it more thought they also reflected around the fact that platforms like Facebook are in dialogue with nation state actors and often have to comply with national regulations, which means that the experience of Facebook in Norway isn't necessarily the same as in other countries. This is something the interviewee had explicit experience of because they are part of an ethnic group experiencing active hostility from a country that Facebook is in dialogue with.

> "Facebook had in their bylaws; they had specified my [ethnic group] movement as something that is not allowed. Therefore, what I'm writing and my mobility on the internet, navigating that is less."

In other words, this interviewee's freedom to express themself on Facebook was constricted by their ethnicity both because of an adversarial state actor, but also because Facebook cooperating with them.

Another social media platform mentioned was Clubhouse, an app with audio chatrooms.

> "There were a lot of trolls [on Clubhouse], because in [Country of Interviewee's Upbringing] you can buy a SIM card without registration. You just go to the store and get a SIM card. So, there were a lot of troll accounts that commented really transphobic stuff and, you know. They'd create huge rooms because it's trolling in a whole other way."

This example illustrated that Clubhouse could be exploited in a way that made it hostile towards trans people. It also referenced how Norway's stricter rules around SIM cards being tied to a social security number can prevent this specific type of harassment, even while removing the choice to be anonymous. The ability to troll in this way was enabled by laxer rules around identification in the country this interviewee grew up in.

Another aspect of using the internet as a queer person that was mentioned was dating online.

> "Every aspect of life is digitalised. Therefore, it's also in somebody else's control. How they ban trans women, for example […] when everybody is on Tinder, and you're not allowed because you're a trans woman. That's where people meet."

Transgender people are reported more often than cisgender people on dating apps (Savage, 2019). Tinder introduced more options for labelling gender on their apps as a partial response to this, but it is still a significant point of exclusion in a world where internet dating is increasingly common, especially for queer people. In a Pew Research Center report, Anderson et al. (2020) found that "LGB adults are about twice as likely as straight adults to say they have used a dating site or app (55% vs. 28%)" (p. 6). It is difficult to find statistics on the prevalence of trans people internet dating, but it is likely to be similar, since the

underlying reasons for internet dating being necessary are the same: small dating pools and ability to filter potential dates beforehand to check if they are actually safe and/or interested.

Surveillance was another vector that reduced feelings of safety connected to being online.

> "There came a report from [national security agency], that they register [people from my ethnic group]. Like, literally, who they are, what they do, where they go, and the best way to do that is digitally."

As already mentioned previously, many interviewees conceptualised Norway as "safer" than other countries (see section 5.3.1). This meant that they often had specific thoughts about travel.

> "My worries about going to [parent's country of origin] would be being visibly queer and not speaking the language. […] That's also why I'm not shaving my head, trying not to dye it, is in case potentially one day I want to go to a place where being visibly queer is not a good move. […] I think if they do look me up, they will find something, even if my FB is hidden. I don't think it's hidden enough to be...yeah. Like they can find my pronouns in my IG bio."

> "It's absolutely something I've thought about. That if I was to travel somewhere where it isn't allowed and they did an internet check on me, then they'd easily figure out that I'm queer. If they search my name. I think. Especially if my Instagram is open."

Being "visibly queer" (hair style, piercings, tattoos, fashion choices, public displays of affection with a partner, etc.) while walking around was one aspect of this, but information accessible online was another that multiple interviewees had thought about.

Two interviewees had specific measures they put into place when travelling, which involved using a "cute", "crappy" or "dumb" phone. "Cute" meaning a phone that only had innocuous content that wouldn't raise suspicion if checked at a border.

> "When I travel, I freshen my phone, no pictures, no accounts. I take it off and then I have cute pictures, like landscapes and flowers. I 'cute-ify' my phone when I travel to [adversarial country]. Because they will check."

Once in the country, the same interviewee would then buy a "crappy" phone (what would usually be called a feature phone or a simple phone, the type of mobile phone that has little to no internet connectivity, more commonly used before the advent of the smart phone around 2010).

> "When I travel to [parent's country of origin] I buy a crappy phone."

The "crappy" phone would be used to make calls and conduct personal business. The "cute" phone would be used to build a picture of a regular tourist trip. The "crappy" phone would then be discarded before the return journey.

> "I buy a new phone there and I use that for calling and things like that. I don't use my cute phone. My cute phone, I take pictures when I'm outside a monument. Like, 'hey, this is a statue', because I need to have proof of me being a tourist on that phone. And then I just throw the other one away."

Another interviewee reported a similar set of tactics, plus scouring their PC. They described this as leaving their gayness behind.

> "I switch out smart telephones with dumb telephones [when travelling]. The old ones, Nokia and so on. I wipe my sensitive information from my PC, if I'm travelling to, for example, [country of upbringing]. All my gayness is left in Norway."

Even with increased vigilance while travelling, an interviewee still described using a dating app to come into contact with other people in the queer community, even if they didn't go so far as to meet up with people, since unknown dating app profiles can turn out to be someone else than who they say they are (see more in section 3.3.3).

> "I sometimes get curious about Grindr [...] then I log on. When I've travelled. For example, to [country of upbringing]. But I never agree to meet. I just chat and check what the situation is like, the community. But I never dare [to meet up]...are you crazy? Suddenly there's five police officers standing at my door […] It can also be militia, terror groups, sleeping cells. And suddenly you're beheaded. Not exactly what you want on holiday. [...] It happens to activists a lot. When they travel to [country of upbringing] or the Middle East or even Russia."

From the answers given by interviewees, it is clear that queer people also have extra considerations when travelling that are exacerbated by digital technology. This is especially relevant for queer people of colour because they often have ties to multiple countries and may be picked out while crossing borders due to both racism and queerphobia.

The internet can be a vehicle for spreading unwanted content, something that is particularly sensitive for a queer person online. An interviewee recounted the story of a person they knew being blackmailed over a video that had been filmed without consent of them having sex:

> "That guy pressured the person I know for money, several hundred thousand. 'I don't have that shit.' 'Okay.' He uploaded it on Pornhub. The other boy killed himself."

This example is both tragic and could not have happened without the capacity of the internet to spread content. It is also likely that the person in the video being queer contributed to the outcome because they weren't open about their sexuality.

Another incident that contributed to fears around sexual video content stemmed from an interviewee being sent sexually explicit videos with ambiguous origin, which lead to questions such as, "How did this end up in Norway? And how did I get it on WhatsApp from a Norwegian guy? Does he know that his film ended up in Norway? Is he Norwegian?" This seemed to cause fear of the same thing happening to the interviewee.

The same interviewee summed up their feelings about content on the internet in this way:

> "It lives its own life. To throw a picture or video onto the internet is like throwing a bottle with a letter in it into the sea. You never know. You don't know where it will reach or end up or which beach it will stop on."

Interviewees brought up a varied set of incidents and situations that made them feel unsafe. They also had many ways to deal with threats to their safety, which will be outlined in the next section.

5.3.3 Safety as doing

The five interviewees had varying ways of dealing with incidents or lack of safety online, which have been grouped into the subtheme 'safety as doing'.

A repeating pattern when asked about what they would do if they experienced a security or privacy breach was that interviewees expressed not being sure. Some of them felt confident that they had someone in their social circles that had the required knowledge and were willing to defer to perceived expertise. An answer that exemplified this was the following:

> "I feel like I do know some people that I would ask [if I experienced a security breach]. […] I have some friends that are programmers or that work in IT in one way or another."

All of the interviewees expressed feeling in some way that they didn't have the necessary knowledge to deal with breaches or feel fully confident that they were keeping themselves safe online. Most of them had still tried to educate themselves on topics like privacy. One interviewee mentioned having to learn about GDPR for work. Despite many interviewees expressing insecurity around their ability to keep themselves safe online, they all had varied and often creative tactics, occasionally subverting tools for their own uses.

The safety tactics interviewees described were varied, sometimes preventative, sometimes reactive. All the interviewees mentioned common measures such as antivirus software, changing privacy settings on social media accounts to reduce tracking, using passwords and PIN codes, changing passwords often, not sharing passwords, not using public Wi-Fi networks, refraining from clicking strange links in e-mails, and multifactor authentication. Changing passwords was a measure that was often used both preventatively and reactively. Multiple interviewees mentioned changing passwords after some sort of breach or in preparation for an incoming harassment campaign when they had done something that would increase their visibility. For example:

> "I try to change my passwords a lot and [make them difficult]. I do that every time I know I'm going to do something in the media, I change."

All the interviewees were between the ages of 23-33, so most of them had some experience of technology in their teenage years, although social media was just in its beginnings and smart phones weren't a thing yet. There were several interviewees who remembered having to navigate using technology while living at home with their families and not yet open about their gender/sexuality. They had a few strategies to deal with that. Examples:

> "I would clear my search history and have certain documents or files hidden in obscure places with a random name or something, so that no one would think of going in there and looking for anything. […] And then at some point I got an external hard drive to save stuff on. I also saved some files on that as well. I'd mask favourite bookmarks and files and delete search history."

> "I'd hear my father come. Sometimes he'd try to walk quietly, but I'd hear. He'd check if I was actually doing my schoolwork and I'd change the window to Microsoft or to TV.no. I always erased history when I went to things that I didn't want my parents to see."

> "When I was in the closet, I would use some anonymous emails for whatever forum, to read about issues."

As mentioned earlier, one of the interviewees experienced a person from their family's ethnic community using information from the internet to harass them through their parents when the interviewee was younger. A tactic they used to prevent the incident from being repeated was pre-emptive blocking:

> "These kinds of things happened, so I had to rethink, sit with my sister and like, you need to tell me about all the people [of our ethnicity] and people that are somehow connected to my family, we need to block them before they find me."

Other common strategies interviewees used was restricting content to certain audiences, censoring themselves online, deleting content, only posting intimate thoughts on certain platforms, or using private accounts. One interviewee explained their reasons for starting to censor themself more online:

> "I used to be really active on Facebook, shared my opinions on wars and racism, but now it's passive aggressive pictures and memes. [...] After several rounds of persistent harassment, especially in the debate about [controversial topic] where me and [my colleague] where harassed for six months by the same people. That specific situation, and death threats and so on, made sure that I'm now careful with what I say on social media."

Changing names online was mentioned by more than one interviewee, it was also mentioned as a common tactic:

> "I changed my name so I could do queer activism. It was also because of other safety things. I think that's really normal. At least among the racialised queers I meet, none of them have their real name in their profiles."

Many interviewees had arrived at multiple types of phone-related tactics related to controlling physical access, preventing their phone number being shared with unwanted people, and not allowing unwanted information to be gleaned if their phone was searched. One example is buying "crappy" or "dumb" phones before travelling and "cute-ifying" a phone, as mentioned earlier. One interviewee also mentioned restricting physical access to their laptop by keeping it with them at all times after an incident where family members had seen something the interviewee had wanted to keep private. There were also other examples, both individual and group measures:

> "I also try to remember to turn off my fingerprint [authentication for phone] when I go to protests, because that's been recommended as a precaution [...] when it comes to interaction with police."

> "When I give my number, if it's on Messenger, I'll write it, I'll tell them they have ten minutes, and then I'll delete it."

> "I started having my phone in my pockets all the time. On silent, no vibrate because vibrations also make a sound. And turned it off when I wasn't using it and put it away. And I had to have a code when the other guy [I was dating] called. That he asked a question that had a concrete answer that didn't have anything to do with the question."

> "When we meet, we collect all the phones and we put them somewhere else. No one is allowed to have their phone in a meeting, regardless of the meeting."

Another tactic when it came to phone usage was misdirection. An interviewee explained that they would either turn off their notifications or, if they still wanted to be alerted, they would make sure the notifications didn't betray any information.

> "When I'm in a meeting I always have [my phone] face down. When I meet [people and] I don't want them to see who is chatting to me. I don't have bubbles coming up, messenger bubbles. When I had that and I still wanted to get notifications, I changed the name of the group chat. They were helping me with certain things, and I changed the group photo, so it was like family and a flower […] I tried to mislead."

Interviewees also took advantage of in-app features on their phones, such as the ability to put sensitive photos into a hidden folder in the Apple Photos app or using timed disappearing messages on Signal (an end-to-end encrypted messaging app).

An interviewee explained that even though the general advice when experiencing a wave of harassment and threats online was to log off and not engage, they still felt the need to be somewhat aware of the situation. They would solve this by asking friends for help or using alternative accounts.

> "Sometimes I use my friends, [I ask,] 'can you just check this account once in a while?', because for safety, in real life, you need to have control of safety online."

> "At least, I will deactivate my FB, that will happen. And maybe use my other FB. Just to see, because I don't want people to tag me, and find me, and write in my message box."

An interviewee explained the process they go through when they know they are about to get attention on the internet: "It depends. I have an account that's connected to different e-mails. I do it through maybe a VPN. Another thing that I do is, as an activist, I think it's really important to have control of what the neo-Nazis are doing, for example. So, I follow them […]. I would never ever dare to follow them through my real name, because I know that's dangerous." They use anonymous accounts to avoid potential harassment, but also to keep track of groups that are dangerous to them.

Another way of dealing with harassment and threats was also the police and government instances. This ranged from reporting incidents,

> "I have been tried to be hacked before. I have been in contact with police because of that.",

to receiving help from the police to hide the interviewees' identity,

> "I had to move, I had to change name. There are two different [types of] police help you can get [in that situation]. Either you need to move from the country, it's huge, but the other one is that I don't exist in certain systems.",

or having code words to alert friends to contact the relevant authorities while travelling,

> "When I travel [...] I have safety words for my friends. Like, "oh, we played chess" and that means something. 'Oh my god, the queen did this and I made a bad move here and here and the king came,' and that means […] you need to call the police; you need to call the Ministry of Foreign Affairs to help me get out of here."

As outlined earlier, queer people are more likely to date using the internet. Tactics around using dating apps were especially reflected in the answers of one interviewee and their experiences with Grindr (see section 1.3). They took measures such as sending naked pictures with a time limit, which was only possible using a premium subscription. The interviewee reflected around the fact that Grindr features that let the interviewee feel safer, such as setting a time limit on pictures, were inaccessible to some people who might need it due to the price point.

The same interviewee also talked about the kinds of evaluations they do when communicating with people using the app. They had warning signs they looked out for that let them know when to refuse to continue communications, such as being asked to move over to a different medium too early.

> "And when almost all of these accounts ask me for my WhatsApp in their fifth or sixth message, then I think 'huh, no, I don't want that, we can just chat here'. [...] Why should I give my WhatsApp? Maybe WhatsApp is less secure? When they send me a file and I open it they can spy on me. Or get information, credit cards, whatever from my phone. That in itself is very dangerous. They want to move the conversation from one app to another that is less secure."

They also outlined a situation where they decided not to meet with someone to have sex because of the way that the potential sex partner (PSP) talked about the interviewee. The PSP used language that the interviewee read as potentially signalling behaviour they didn't want from a sexual partner. They then reacted like this:

> "So, I thought, that'll be rough, that's going to hurt, that'll be brutal. So, I sent a message and said 'Hey, I can't.' Because I didn't feel safe. Exactly because of the way he used social media to approach me."

Grindr was the conduit between the interviewee and the PSP, but the way the PSP communicated allowed the interviewee to decide to preserve their own safety.

Another way the interviewee used Grindr has already been mentioned earlier. The interviewee uses Grindr to come into contact with community when travelling to certain countries where being queer is criminalised, but they don't meet anyone in order to stay safe.

> "I sometimes get curious about Grindr [...] then I log on. When I've travelled. For example, to [country I grew up]. But I never agree to meet. I just chat and check what the situation is like, the community."

Most of the tactics that have been outlined have been for defensive purposes, but interviewees also mentioned tactics that were used for other reasons. There were fairly everyday things like using a VPN (Virtual Private Network) primarily to gain access to geoblocked content (content that is only available in certain geographical locations), but there were also other examples.

One such example was an interviewee that circumvented Facebook's moderation to post political content.

> "I told my friend, there was this picture and you're not allowed to have [important political figure] as a Facebook picture. But if you want to have him in the background and you are in the front and [he's] not in focus, then you can get away with having that."

Another example was an interviewee using anonymity online to surveil and "troll" far-right extremists they wanted to keep track of.

> "I have an account that's connected to different e-mails. [...] as an activist, I think it's really important to have control of what the neo-Nazis are doing [...] I would never ever dare to follow them through my real name, because I know that's dangerous, but when it comes to these kinds of things, sometimes I want to troll them."

There were multiple interviewees that mentioned using anonymous accounts to keep track of people. This shows that even though the lens of this thesis might be about queer people of colour as 'marginalised' or 'under threat', they still have their own priorities outside of just defending themselves or staying safe. Sometimes they use creative solutions to avoid censorship and to keep track of people they deem as dangerous.

Queer people of colour have a variety of tactics that they use to stay safe online, the next section will outline the ways that staying safe is a constant cost-benefit analysis for queer people of colour.

5.3.4 Negotiating safety

While talking about safety, how it can be threatened, and attempts at maintaining it, a thing that came through repeatedly was the fact that there were no easy answers. Often, the same platforms that were exposing interviewees to potential danger were the same places that were allowing them to seek safety with community. Trying to maintain safety was a constant negotiation, sometimes the 'safest' option wasn't practical or possible. And sometimes it was just too inconvenient.

There were cases where practical considerations got in the way of safe practices, such as one interviewee not being able to use multifactor authentication anymore after sending their laptop away to be repaired.

> "Used to have a fingerprint, but my laptop doesn't let me configure the fingerprint or PIN code, only the password, since I sent it in [to be repaired] when it broke."

There was also an anecdote about a time an interviewee tried to secure their images using a password protected vault, but that backfired when their phone broke and was replaced.

> "I used to have this folder vault for sensitive images, but then I lost my photos from my other phone [...] because instead of fixing my phone they just gave me a new one because of the warranty."

The interviewee said they stopped using the password protected vault after that, since they didn't want to lose their pictures again. This is indicative of the kind of obstacles that can stand in the way of people doing things the most 'secure' thing, because security can be outweighed by other considerations, such as the need for redundancy or convenience.

The interviewee that talked about having to move and change their name in section 5.3.2, expanded on how having to hide their identity affected their life. The interviewee had to hide their identity due to a young queer person's family turning up at the interviewee's door after finding communication online. The process of hiding their identity made other things in their life more difficult, even though it was a measure to increase safety. Another layer to the story

is the fact that the high level of inconvenience experienced when having to hide identity in this way is partially due to Norway being such a highly digitalised country. The majority of public services are connected to a social security number in some way. The way that digital technology weaves into this interviewee's story shows how contextual and nuanced safety can be.

> "It's so much and because of that it's so difficult. I can't buy things on invoice as a private person because they can't find me. [...] The safety sometimes goes too far. Just easy things, like when I move, I can't just do things in Altinn [a Norwegian government portal]. Everything I have to do; I have to do through the police. [...] There are so many things I can't do that is easy access for normal people, because of my situation. I need to do everything analogue. And I need to go to the fucking police every time. I can't go to NAV [Norwegian public welfare agency]. NAV can't find me and sometimes I need help. Direct help. I can't even get the vaccine. I have to do it through a whole different system than you guys."

Almost all the interviewees expressed mixed feelings when asked whether they felt they could stop using social media. They often seemed to wish they could but also didn't see it as realistic. This was exacerbated by the fact that social interactions had been completely changed by the COVID-19 pandemic. One interviewee recounted an attempt to delete a social media account:

> "I deleted Instagram for one night and I felt really isolated, especially now [during pandemic], because I haven't seen people at all. That's the only place that I really get updates from my friends."

Multiple interviewees also expressed an inability to leave social media due to their involvement in the LGBTQ+ community. Two different interviewees talked about their jobs making it necessary to be online:

> "I do feel like I deal with not wanting to be completely on social media, but finding it difficult to leave, in a sense. Especially when it comes to Facebook. I'll just straight up say Facebook because I use it for a lot of work-related things."

> "I'm in a job that requires that I'm on social media. Because I communicate with people that are unsafe, people that are in the closet."

There was also a sense of inevitability for some interviewees. One interviewee expressed the futility of trying to go offline because their information is already out there:

> "I don't know, because it sometimes feels like the only safety is not existing online, but there's already so many traces of me on the internet."

Another reason for it being hard to stay offline was feeling a lack of control over what was happening. This was specifically in connection with logging off during harassment campaigns.

> "I get stressed by not being online as well. Because then I don't have control."

One of the interviewees explained the double-bind they were sometimes put in due to their job. They worked at an organisation where they often interacted with queer people of colour and had reflections around the nuances of trying to gather data about a group that is small and easily identifiable. A dilemma that has also been faced in the research done in this thesis.

> "Especially in my organisation, we have to be even more careful in how we handle information and how it's presented and used – for example in research or surveys or stuff like that […] it can out someone pretty easily and potentially endanger them as well. Especially for our community it's very important […] a lot of measures made to improve people's lives are based on science and research and it's hard to gather the correct data and necessary information, when the same information endangers people, so you have to be really careful. And also, you're dealing with people that don't want to be identified in any way, so they often don't necessarily partake in these kinds of things, so it goes both ways and makes it very difficult."

Other examples of negotiations around safety being done at work have already been mentioned, where an interviewee described their organisation's procedure for coming into contact with queer people who needed help. Initial contact would often be through social media but would then be moved offline in a crisis for increased safety. An example of the potential consequences of online communication was outlined earlier, where an interviewee was trying to help a young queer person and family members of the youth showed up at the interviewee's door after getting access to their communications. The interviewee had to change address and name. These examples show that there is an ongoing cost-benefit analysis between getting into contact with people who need it and maintaining personal safety.

Sometimes one person's personal safety can depend on that contact, while putting the receiver of the contact in danger, so it's never a straightforward assessment.

Many of the interviewees talked about negotiating different levels of openness regarding their gender and/or sexuality online, both in the past and the present. 'Coming out' is often seen as a one-time event but is usually more nuanced in reality. People might be open in some social contexts and not others. Some people might not be at all interested in 'coming out' in the way it is popularly understood, an explicit announcement to the world at large. Openness around gender and/or sexuality is therefore more of a negotiation than a one-off decision. These nuances translate to the ways that queer people navigate online.

An interviewee recounted the way they had navigated the popularity of having personal websites when they were younger.

> "I do remember when I was younger […] you could kind of make your own personalised website. […] I remember that a lot of my friends and people at my school were part of those things and I never was because I felt like it was too personal and even if I were part of something like that, I couldn't really be myself on those platforms, so I just wasn't on them. [...] It was weird because, of course, I could just fake it or I could just put out the content that wasn't related to my identity, but for some reason I felt like it was very invasive and when I saw other's content and what they'd put out it was like "oh, I'm talking to this person" and blah, blah, blah. I guess it was also related a lot to relations and that was also something I struggled a lot with, having good relations to friends that were on a deeper level or to people and classmates in general."

This anecdote is an example of the way that technology has taken on a larger role of facilitating people's communication of their identity to the world. Navigating that as a young queer person can be difficult, as stated by the interviewee. Both because there is a fear of exposing too much information, but also because the inability to be fully authentic in the way that is often encouraged on these platforms makes participating difficult.

As already mentioned earlier, a tactic that one of the interviewees used when on Grindr was timed deletion for pictures they sent to others. This interviewee also mentioned that they didn't send pictures before being open about their sexuality, which gave them a better

understanding of people who couldn't use pictures on their profiles. Deciding whether or not to use pictures is the kind of negotiation that many queer people have to make online. On the one hand, it is safer to have more pieces of verifiable information if planning to meet up with someone. On the other hand, it can be dangerous to send identifiable information if it can out someone who isn't open.

Another way of negotiating safety was varying behaviour on different platforms and controlling the visibility of content. As already mentioned earlier, one of the things that could be avoided by picking the right places to communicate different things was context collapse. Interviewees dealt with this in different ways. One interviewee had differing approaches to Instagram and Facebook, feeling more comfortable being open on the former.

> "I'm definitely more open on Instagram. [...] It's definitely easier for me to be, not even just openly queer, but just posting things in general. They go hand-in-hand, I suppose."

> "With Facebook, I never know how they will gender me if they comment, so I just don't bother."

Another interviewee had decided to make their Instagram completely open, even knowing that makes information about them being queer publicly available. The same interviewee said earlier in their interview that they had made their profiles private and deleted a lot of content for a few years preceding this decision.

> "My Instagram profile is public now and there's lots of Pride pictures there. So, now it's very available. Everyone can see that I'm queer."

Several interviewees mentioned the police in different capacities. The police were often brought up when talking about ways to deal with incidents, but most interviewees also expressed ambivalence or seemed to see the police as a potential source of threat. At the same time, the police were often the only option mentioned once things had escalated to serious threats and harassment. Even so, interviewees didn't always seem to feel that police intervention ended up particularly useful. As already mentioned earlier, one of the interviewees had specific tactics when going to protests as a precaution to prevent police

access to their phone, this suggests that the police were seen as a threat in that specific instance.

Another interviewee talked about trying to gain assistance from the police, but only getting a limited amount, with the police apparently directly admitting that they could only help so much, "When I went to the police for help about the harassment and attempted hackings, they […] said it to me directly. Like, 'sorry, we can't help you so much, but we can do this and that.' It's shit."

An anecdote about differential treatment from the police showed some frustration about the limited set of solutions that they provided to the 'average' person. This, again, highlights the ambivalent relationship to the police, who are seen as an instance to keep people safer, but didn't necessarily seem to make the interviewee feel much safer.

> "Me, a politician, and a friend of mine got hacked. […] And the politician, a white Norwegian politician, got the police around her house to check on her safety, on and off. They had a car outside to see who's coming to her door, because we all got death threats. […] The police were just like 'get a new phone, get this and this, do that' [to us]. The same attacks, the same threats. […] I know why they did that, but it's wrong. We should have gotten equal treatment. We were receiving the same threats."

Another anecdote where an interviewee seemed to have had a less than satisfactory outcome when going to the police was this one:

> "The police closed the case because they couldn't find out who was behind that profile. […] And when the police close these types of serious cases, then you become really careful. And it affects your life. And it changes how you behave in your daily life."

The police were sometimes also framed as a direct danger to queer people of colour, using digital technology to especially surveil undocumented people.

> "Being queer in Norway, of course it can be dangerous, but when you add geopolitics and asylum and all of these things, when people are undocumented. If these things are added, it's not safe at all. And the police are hunting down undocumented people,

> queers, here [in Norway]. How do you do that? It's through the internet, because everyone leaves traces there, everyone is using it."

Interviewees made it clear that safety was a negotiation they were constantly engaged in. To round up the interviews, interviewees were asked about ways they thought safety could be increased for queer people of colour. Their responses will be outlined in the next section.

5.3.5 Envisaging safety

Interviewees often made asides about things they wished were different. This could be something as simple as complaining about Apple's inconsistent functionality around hiding images in the Photos app:

> "I wish [the hidden image folder] was password protected. I don't know why it's not. Why have a hidden folder if you're not going to make an effort to actually protect it?"

Multiple interviewees also expressed a desire for tech companies to take more responsibility for the things that happen on their platforms. Or, at least, for there to be someone that takes responsibility.

> "Facebook is not responsible for hatred. It's a media, but it isn't moderated. We need someone who has the responsibility. Nobody knows how to contact Facebook, it's super weird."

> "[I want] more policies and rules for the big tech companies. That they take a stronger stand on not accepting racism and homophobia on their platforms."

One interviewee, who experienced the Vipps stalking episode outlined earlier, also expressed a wish for payment apps that weren't so tightly connected to actual identities, comparing with Norwegian options with the larger set of payment app choices in the US such as 'Cash App' and 'Venmo', which do not require people to use their real names. They seemed to think that part of the reason that there are less choices for anonymity in Norway was down to lack of scepticism, something that could possibly be true when taking into consideration how most interviewees conceived Norway as safer than other countries.

> "People are more sceptical [in the US] as well. Here we are, like, trust everything."

Interviewees were also asked explicitly about things they wished for to make technology safer for them. The last question in the interview was: *Could you think of any strategies/tools that don't exist that could make using technology safer for you or other QTIBIPoC?* Interviewees had a varied set of responses.

One expressed desire was for lower barriers to knowledge. As most of the interviewees expressed not knowing where to go for security knowledge at several points during their interviews and their security practices seemed to be put together in a fairly ad-hoc manner, this seems like a solution that would be helpful for multiple people.

> "An accessible overview of internet security. A lot of tech stuff isn't really accessible to people who don't know tech stuff. People who work in tech get so easily annoyed when non-tech people take a little bit longer to get it. Also, often [using] language that is inaccessible to people who don't know it."

Another interviewee focused on the need for existing platforms to take more responsibility for harassment that happens on their platforms. Gaysir is a Norwegian news and social networking site targeted towards LGBTQ+ people.

> "When you go to Gaysir and go to the forum, the way they talk about [colleague] there... I think it's Gaysir's responsibility to clean up, so that the people who see what [colleague] is going through and think 'damn, this is not okay'. Then they can see that there's still someone addressing the issue and that it's safe for them to participate in the debate. Platforms need to take more responsibility."

Two interviewees suggested platforms exclusively for queer people of colour to interact. One interviewee especially had in mind an app that wasn't easily detectable so it could be used by people who need to be discreet, especially those living in countries where being queer is criminalised.

> "Making our own platforms. For example, a Grindr that's for black and brown people only. [...] For it to be safer. For it to not be so fetishizing. For there to not be racism. For the conversations to be valuable and good. Then we need to have our own platforms."

> "If there was a way to have a super safe programme or app or way to interact with people. […] if you're in the closet or not, but you know that they're queer and that it's

> very safe and you can interact and share stuff with people, like queer people of colour. […] I'm thinking for people that live in countries where you can't be yourself, where you could be prosecuted for being yourself. […] Like, even if the government or whoever saw the app or check it, there would be no way to figure it out. Maybe it could even be hidden in some way."

The next suggestion is relevant to the two previous ones, because trying to create spaces specifically for queer people to interact brings with it the problem of vetting who gets to join the spaces. A problem that becomes harder when considering the fact that many queer people aren't open about their identities and therefore have a need for anonymity. As the interviewee mentions, trying to verify people's identities has both pros and cons, but it is a question one has to consider if trying to make spaces predicated on a shared identity. Lack of anonymity has risks, but so does allowing people who potentially have bad intentions into spaces that are supposed to be safe.

> "Something to secure people's identities. This is two sides of the same thing. If you're forced to identify yourself, it can be misused. But if there was a closed group for racialised people and a neo-Nazi suddenly got in who'd pretended to be someone else, that would be dangerous. But how do you make sure that doesn't happen? Then you have to make sure you know who's in the group."

Another interviewee had thoughts more in the direction of political movements and activism around digital safety. They seemed to be missing a grassroot approach to the issue of digital safety. They did not see the current options, such as the police, as currently being good enough.

> "The internet is not safe, it's really not safe, and I want tools. I want a movement of activism. In the same way we have, for example, a movement against femicide."

> "Like an NGO [non-government organisation] for a start, at least, but […] the police should be better. This should be public knowledge. It should be as normal as libraries these days because this is what the world looks like. People need to go to a place and not Google and find products to buy, but real knowledge. These are things that need to be learned in school, early. In the same way they learn how to do other things. [...] We need activists around this, that is what we need, a civil movement almost."

5.4 Summary of findings

The thematic analysis process resulted in one background theme, ‘intersectionality’, and one overarching theme, ‘safety’. The overarching theme included five subthemes: ‘mental models of safety’, ‘threats to safety’, ‘safety as doing’, ‘negotiating safety’, and ‘envisaging safety’. The following sections will summarise the findings from the different themes.

5.4.1 Intersectionality

Intersectionality showed up as a theme throughout interviewees’ responses, it was therefore chosen as a background theme since it was interwoven into all the subject matter. Interviewees saw intersectionality as increasing risk in different ways. Engaging in intersectional activism was more dangerous than single-issue activism, being a queer person in Norway was more dangerous when that person had multiple overlapping marginalised identities such as being undocumented, doing research was more sensitive when researching queer people with multiple overlapping marginalised identities since it made it more difficult to anonymise respondents, and multiple interviewees thought they would be less afraid, or in less danger, if they had less overlapping marginalised identities.

5.4.2 Mental models of safety

Mental models of safety as a subtheme comprises interviewee’s perceptions of safety. It is important to understand the way interviewees thought about safety to have a holistic view of the rest of their responses. Interviewees mentioned common concerns when it came to their safety online, such as viruses, spam e-mails, and how big tech companies use their data.

Interviewees that had experienced harassment online tended not to see tech platforms as their largest problem, comparing them favourably to, for example, “radical fascist platforms”. All interviewees expressed concerns about online harassment and often knew someone else that had experienced it, even if they hadn’t themselves. Multiple interviewees had experienced harassment online and this had left lasting effects on their sense of safety. Interviewees frequently expressed that safety online was impossible to separate from other areas of life. For example, online dating was a situation that made one interviewee felt particularly unsafe. Trying to vet sexual partners was seen as more challenging due to the additional factors introduced by communicating online.

Interviewees frequently expressed resignation when talking about dangers online, seeming to see them as unavoidable. They would simultaneously refer to themselves as “careless” or state that they should learn more about certain issues, so it seemed they weren’t satisfied with their current situation. Interviewees often seemed curious once security related topics came up but gave an impression of not knowing where to go if they wanted to find more information. An example multiple interviewees came back to when asked about security was banking, which seemed to be a mental reference point when it came to safety procedures that were easy to follow.

Interviewees had different categories of situations they deemed as unsafe, drawing lines between “direct hate speech” and “uncomfortable messages”, for example, even though both categories qualified as feeling unsafe. Feelings of safety when using social media were also affected by factors like social proximity and shared identity markers. Interviewees generally felt safer when they knew who was seeing their content, although this wasn’t always the case due to context collapse.

Interviewees talked about creating “safe spaces” online through their work, which involved active moderation, and used those online “safe spaces” to move communication from being online to physically meeting face-to-face in crisis situations.

5.4.3 Threats to safety

Threats to safety as a subtheme comprises responses interviewees made that outlined which online incidents they perceived as unsafe. A large factor that seemed to affect whether interviewees had experienced hostility online was to do with whether they were politically active.

Interviewees recounted average incidents such as spam e-mails and logins from unknown users, but it wasn’t always easy to write incidents off as random. Interviewees with previous experiences of harassment found it hard to differentiate between random and targeted attempts at hacking. Interviewees had experienced targeted hacking, harassment, death threats, and rape threats, usually connected to being visibly political online. At least one interviewee had to change their name and address due to the consequences of working with queer people of colour and communicating online. This exemplifies the way that digital safety is impossible to separate from physical safety, which multiple interviewees mentioned.

An interviewee had concerns about revenge porn (the spreading of sexual content without consent of the persons involved) due to having seen it happen to people they knew. One of the interviewees also recounted a stalking incident, where someone communicated with them through Vipps, a mobile payment app, even though they had been blocked on all other platforms. Multiple interviewees talked about experiences from when they were younger and not yet open with their families about their gender and/or sexuality. They recounted incidents where technology was a door to unwanted information being shared with family members.

Far-right extremists were seen as a potential threat by all the interviewees, even those who hadn't experienced any direct harassment. One of the interviewees used anonymity to keep track of far-right groups online. Social media platforms were perceived with scepticism. Interviewees didn't trust platforms to take care of their privacy and also modified their behaviour on platforms to prevent unwanted incidents, such as misgendering. Censorship on social media platforms was also something interviewees had experienced. Tinder was brought up as an example of an app that had functionality that could be hostile to trans people, because trans women are often reported.

Technology was seen as a surveillance mechanism that could put queer people in danger. In Norway, the worry was that authorities could use it to track people, especially if they are undocumented. Outside of Norway, interviewees talked about having to protect themselves when travelling to prevent unwanted information being found on their phones or laptops during border crossings to countries that may criminalise queer people or discriminate the interviewee's ethnic group.

5.4.4 Safety as doing

Safety as doing as a subtheme comprises the responses that have to do with concrete tactics interviewees used to maintain safety.

Interviewees expressed not feeling like they had the necessary expertise to protect themselves in the case of a breach, which meant some of them planned to go to people they knew who they felt had more knowledge. Despite this, they still shared a diverse range of tactics they used to try to stay safe online. This included measures like multifactor authentication, anti-virus software, and changing their passwords before they knew they would get a lot of attention in the media.

Interviewees also recalled tactics they used in their younger years before they were open about their gender/sexuality to their parents. These were less formal measures, such as deleting browser history and giving misleading names to bookmarks and folders. A tactic used by one interviewee was pre-emptively blocking people in their ethnic community to prevent them seeing online activity and reporting it to the interviewee's parents.

A tactic many interviewees used was restricting content on their social media profiles, this included making their profiles private, choosing which audiences saw what, censoring themselves, and deleting content. Interviewees also changed their names on their social media profiles so they wouldn't be tied to their real identities, which one interviewee said was common for the queer people of colour they knew.

Interviewees had a lot of tactics surrounding their phones. The goal of the measures was to prevent physical access by unwanted people, keep phone numbers private, and prevent tracking via GPS features. Interviewees also used in-app features, such as hiding sensitive pictures in the Apple Photos app or timed disappearing messages in Telegram. Interviewees also mentioned attempts at direction such as renaming chats and using innocuous pictures to mislead anyone who saw notifications on-screen.

When experiencing waves of harassment, interviewees would be advised to stay offline, but sometimes still had a need to keep track of what was happening. They would then use their friends or alternative profiles to monitor the situation. Most interviewees that had experienced serious harassment said they went to the police when it happened, in one case resulting in an interviewee having to hide their identity.

Interviewees also mentioned using code words to communicate. One example was an interviewee travelling to areas in unstable geopolitical situations who wanted to let their friends know if something had gone wrong. Another example was an interviewee that had a code to let their romantic interest know it was actually them answering the phone.

Dating apps were also a place that interviewees used tactics around. This could be using in-app functionality such as sending pictures with time limits, evaluating sexual partners via the way they communicated online, or deciding not to meet up with people in countries with queerphobic laws even when they were using apps to get into contact with the queer community.

Interviewees also mentioned non-defensive tactics, such as using VPNs to access geoblocked content, intentionally manipulating pictures to circumvent Facebook's moderation, and using anonymous accounts to keep track of far-right extremists.

5.4.5 Negotiating safety

Negotiating safety as a subtheme comprises the responses that had to do with safety being a complex negotiation that required interviewees to weigh different risks when deciding what to prioritise in their decision making.

Interviewees mentioned practical barriers to making safer decisions, such as malfunctioning technology or a photo vault app that was so secure the interviewee wasn't able to transfer their pictures to a new phone when their old one stopped working. Another interviewee outlined how their hidden identity had caused problems for them, from losing access to the Norwegian public welfare agency (NAV) to a much harder process when trying to receive vaccines.

When asked whether they felt they could choose not to be online, all interviewees said no. Reasons included social media being their primary source of community (which was exacerbated by the COVID-19 pandemic), needing to stay updated on things happening online, and having to be online for work related reasons. Multiple interviewees had jobs where they were in regular contact with queer people of colour and reflected around the kinds of cost-benefit analyses they had to do while working. This could be trying to figure out how to do research that ran the risk of outing people due to QPoC being a small, easily identifiable group and deciding when to move communications offline for increased safety.

Multiple interviewees also had reflections around negotiating different levels of openness about their gender and/or sexuality online. An example of this was an interviewee who chose not to participate in making personalised websites when they were younger because they didn't feel they could be authentic. Another example was an interviewee who didn't use pictures on dating apps before they were open about their sexuality. Other interviewees communicated differently depending on which platform they were on and whether they knew who was in their audience.

Another point of negotiation that came up multiple times was the police. Interviewees mentioned the police multiple times as a solution if harassment and threats escalated online but seemed to have had mixed experiences with how helpful the police actually were if they got involved, citing closed cases, unhelpful advice, and unequal treatment in the face of serious harassment. One interviewee shared a tactic specifically meant to prevent the police from gaining access to their phone when going to protests and another was concerned about the police using digital evidence to surveil undocumented people in Norway. Interviewees seemed to have an ambivalent relationship to the police.

5.4.6 Envisaging safety

Envisaging safety as a subtheme comprises interviewees' responses related to their wishes for functionality, tools, or measures that didn't exist yet and increased safety.

Interviewees expressed concrete desires to change existing structures, such as password protection for sensitive images on Apple products, social media platforms taking more responsibility for moderation, more legislation for tech companies, and payment apps that don't require connecting profiles to real identities. Interviewees had a few different answers when asked for new solutions that could increase digital safety for queer people of colour. One suggestion was accessible guidance on how to improve security, specially targeted towards people with a non-technical background. Interviewees also suggested new platforms specifically for queer people of colour to use, with one interviewee emphasising a need to vet people's entry into such spaces. One interviewee focused on activism and knowledge sharing, wishing for spaces they could go to get help and learn more about security, for example, a non-government organisation.

6 Discussion

This thesis aims to explore queer people of colour's experiences with digital safety.

To do this, five research questions were chosen:

1) Are LGBTQ+ racialised people especially vulnerable to attacks on their privacy?
2) Are LGBTQ+ racialised people fully covered by existing privacy regulations and information security measures?
3) Which specific unsafe situations are LGBTQ+ racialised people exposed to through use of technology?
4) Do LGBTQ+ racialised people have specific security concerns?
5) Which alternative strategies do LGBTQ+ racialised people use to stay safe outside already existing digital security frameworks?

This chapter will discuss the research questions in light of the results laid out in the previous chapter, highlight some existing solutions to problems brought up in the results chapter, and suggest a possible new solution.

6.1 Research questions

6.1.1 Are queer people of colour especially vulnerable to attacks on their privacy?

As outlined in section 2.2.3, there are documented situations where queer people have had their privacy violated, such as queer people in Nigeria being arrested because of information illegally found on their phones by police officers (The Initiative for Equal Rights, 2019) or young queer people being outed to their families without their consent due to surveillance software flagging search terms at their schools (Caraballo, 2022). The results outlined in the previous chapter suggest that queer people of colour are vulnerable to attacks on their privacy specifically because of their identities, with the most extreme result being a person having to change their name and address due to an incident connected to their work with young queer people of colour. The results also suggest that queer people of colour are especially vulnerable to attacks when they are politically active.

6.1.2 Are queer people of colour fully covered by existing privacy regulations and information security measures?

There is a short discussion of Europe's General Data Privacy Regulation in section 2.1.4. Under GDPR certain categories of personal information, such as race, ethnicity, or sexual orientation are categorised as 'sensitive' and gain extra protection. Gender is not one of those categories, which means that a significant segment of the queer community does not qualify for this extra protection. The violations of privacy outlined in the results chapter suggest that even if there are privacy regulations, they might not be fully effective in preventing incidents. When it comes to information security measures, the responses from the interviewees in this thesis do not point to especially egregious information security breaches. However, there were still some incidents such as the interviewee that had been stalked through Vipps (a Norwegian mobile payment app) due to there being no blocking function that point towards information security measures not always being up to scratch. Section 2.3 discusses the lack of diversity in the tech industry and how it might be a contributing factor to the decisions that are made about security when building technology.

6.1.3 Which specific unsafe situations are queer people of colour exposed to through use of technology?

The results chapter lays out the experiences of interviewees, which included hacking, harassment, death threats, and rape threats. One interviewee had to change their name and address after someone physically turned up where they lived. There were also interviewees whose family had seen things the interviewee didn't want them to see on their devices before they were open about their sexuality. One of the things discussed in section 2.2.3 is the way dating apps can be used to lure queer people into dangerous situations (Carroll, 2019; Noack, 2014), especially in countries where being queer is criminalised. Responses from interviewees also suggest that dating apps can be a source of danger, either because people are not who they say they are and/or end up being dangerous.

6.1.4 Do queer people of colour have specific security concerns?

The responses from interviewees suggest that they had concerns specific to their identities even when they hadn't experienced any particularly extreme incidents (at the time of the

interviews). Every interview mentioned far-right extremists as a concern when navigating online. Most interviewees were worried about tech platforms and privacy, which was especially sensitive due to information about their identities potentially being used in a way they didn't consent to. Section 2.1.2 discusses data gathering can have unfortunate consequences. For example, in the case of targeted pregnancy ads hounding someone who's just had a miscarriage (Moss, 2019) or a pregnancy being revealed to a conservative family without permission (Kosinski et al., 2013, p. 1).

6.1.5 Which alternative strategies do queer people of colour use to stay safe outside already existing digital security frameworks?

Even though interviewees expressed not feeling like they had enough knowledge about keeping themselves safe online, they still responded with a varied set of tactics they use to try to maintain safety. Some of them were informal measures from a younger age where interviewees were not yet open to their families, such as deleting browser history and using misleading names for folders and bookmarks.

In the present day, interviewees restricted content on their social media profiles, changed names so their real identities weren't tied to their profiles, and censored themselves. Interviewees also kept their phones close by, changed their numbers ahead of harassment waves, and left their phones behind when going into sensitive meetings to prevent location tracking. Interviewees used in-app functionality such as hidden folders for images and timed disappearing Telegram messages or timed disappearing images on Grindr. During waves of harassment, interviewees would use friends or alternative profiles to stay updated on the situation online. Interviewees that had experienced harassment online said they went to the police once things got serious. Another tactic was using code words in online communication to alert friends to dangerous situations or confirm identity. Interviewees also used tactics that weren't necessarily only to stay safe, such as intentionally circumventing Facebook's moderation and using anonymous accounts to keep track of far-right extremists.

6.2 Possible solutions

The *envisaging safety* theme in the results chapter gathers interviewees' wishes for new functionality, tools, or measures that they felt would increase safety for them and other queer people of colour. The two following sections will discuss possible solutions to those wishes.

6.2.1 Existing solutions

This section will discuss existing apps, websites, and organisations that may be possible solutions or blueprints for possible solutions to some of the concerns raised by interviewees.

Multiple interviewees expressed a wish for apps that were exclusively for queer people of colour to use to be in community together online. Queer Nigerian software developers have built an Android app called Qtalk (Job, 2022). On the Google Play store the app Qtalk is described as: "Nigeria's first social and counseling mobile app for the lesbian, gay, bisexual, transgender, intersex, and queer [LGBTIQ+] community." (*Qtalk*, n.d.). This could be an example to follow.

One of the interviewees also expressed a desire for information accessible to non-technical people. Tall Poppy is a service that aims to give "accessible, step-by-step guidance to digital safety" (*Tall Poppy - How It Works*, n.d.). Members have access to information that allows them to secure their online footprint and prepare for incidents. Tall Poppy seems to mainly be aimed at workplaces (Shieber, 2018), but it could be a blueprint for more accessible resources.

Another desire expressed by an interviewee was for non-governmental organisations where they could gain assistance with digital safety. There are already organisations that work in related fields, some of which do work globally, although none of them are based in Norway.

The *Electronic Frontier Foundation* is a non-profit that "champions user privacy, free expression, and innovation through impact litigation, policy analysis, grassroots activism, and technology development" (*About EFF*, 2007). They have made open-source tools such as Privacy Badger (a browser extension that blocks trackers) and HTTPS Everywhere (a browser extension that encrypts communications with websites), which are free for anyone to use.

Citizen Clinic is hosted at the Center for Long-Term Cybersecurity at University of California, Berkeley. It is a public-interest digital security clinic that aims to help civil society organisations (organisations defending human rights and doing political activism) defend

themselves online (‘Citizen Clinic’, n.d.). This is a blueprint that could be applied in more places, which will be discussed further in section 6.2.2.

The initiatives mentioned are not meant to be an exhaustive list. There are many more working on technological equity, such as Tactical Tech[1], Citizen Lab[2], and the Algorithmic Justice League[3].

6.2.2 Clinical computer security

This section will discuss a possible new solution to some of the wishes made by interviewees.

When interviewees were asked whether they could think of any strategies or tools that could make using technology safer for QTIBIPoC, one of the answers was: "I would like to have activists that one can go to for help. When you have special needs.". An interesting concept that could potentially contribute to helping with this problem is outlined in a paper written by Havron et al. (2019): clinical computer security, where “[t]he goal is to develop, in a rigorous, evidence-based way, a set of best practices for how a technology consultant can assist a victim — called the client in such a service context — with digital insecurity. Best practices will need to encompass a range of issues, including how to setup and run clinics, recruit and train volunteers or paid professionals to staff them, deal with the many legal issues that will inevitably arise, and how consultations with clients should proceed.” (p. 107).

Havron et al. (2019) set up a clinical computer security service for victims of intimate partner violence (IPV) where they could go and receive technical support for issues like “account compromise, installation of spyware, and harassment on social media” (p. 105) with the assistance of a ‘technology consultant’. There seems to be a need for a place people can go that isn’t the police or a for-profit tech support service. As is mentioned in the paper, “case workers, lawyers, police, and other professionals that work with victims report having insufficient tech expertise to help victims with digital threats” (Havron et al., 2019, p. 107). This dovetails with some of the experiences outlined in the results chapter, interviewees had mixed experiences with the police being able to help them during digital incidents. Multiple communities also have fraught relationships with law enforcement and therefore wouldn’t go

[1] https://tacticaltech.org
[2] https://citizenlab.ca/
[3] https://www.dair-institute.org

to them for help. And paid tech consulting services can be inaccessible due to cost (Havron et al., 2019, p. 107).

There is already a precedent for 'clinic' solutions. Law institutions incorporate pro-bono work into their models in multiple places. It is more common in the US, but Norway also has services such as Jussbuss[4], which is run by law students who give free legal consultations, and JURK[5], which gives free legal consultations to women. Why is this not more prevalent in the tech industry? Citizen Clinic[6] at UC Berkeley, which facilitates students giving free security consultations to civil society organisations, might be one example of a blueprint for starting such an initiative. There could be potential challenges of ensuring sustainability and quality with this particular direction, but the dangers people can be exposed to through technology can be just as serious as legal problems – or they can lead to legal problems.

Any sort of clinic solution would have to be carefully thought out and incorporate stakeholders from all the affected communities. Havron et al. (2019) emphasise that they made the choice to work closely with already existing IPV services. This is important because the root problems are not of a technical nature and people who are tech specialists will not necessarily have the specialised domain knowledge needed to understand all the context, which in the worst-case can actually make the situation more dangerous. A bad intervention can be worse than none at all.

A clinic solution would only be one aspect of trying to mitigate the dangers queer people of colour experience, since it does not actually solve the problem of privacy violations and security incidents. As Havron et al. (2019) say, "[o]ne avenue for improving on the status quo is pursuit of new technology designs that better resist such targeted attacks", but it is also unknown whether it is feasible for such attacks to ever be completely eradicated, and even if they were, it would likely take a long time and not be a short-term solution for the people being targeted now (p. 107). No computer security clinic can end racism, homophobia, or transphobia, which are the underlying reasons for specific targeting of queer people of colour, but a clinic could give them somewhere to go when they need help.

[4] https://foreninger.uio.no/jussbuss/om/
[5] https://foreninger.uio.no/jurk/om/
[6] https://cltc.berkeley.edu/about-us/citizen-clinic/

A clinic solution would also likely be well received by technologists who want the opportunity to do good with their skillset. As van der Velden et al. (2021) show, students at the University of Oslo's Institute of Informatics (IFI) "want to engage with social, ethical, and environmental challenges in their future work life" (p. 4). This is likely to apply to more than just the students at IFI.

Extending the research Havron et al. (2019) have started on clinical computer security and making it specific to queer racialised people is a potential continuation of the exploratory work done in this thesis. But any research would have to "respect client well-being, [be] cognizant of safety risks, weigh the relative benefits of research to those risks, and, overall, minimize the potential for harm." (Havron et al., 2019, p. 107).

7 Conclusion

This thesis has explored queer people of colour's experiences with digital safety.

In chapter 1, the research questions, motivation, and terminology for the thesis were introduced.

In chapter 2, information privacy, information security, and the way diversity affects outcomes in the tech industry were explored using literature in the field to build a background for the rest of the thesis.

In chapter 3, the four components of the conceptual framework for this thesis were outlined – experiential knowledge, intersectionality, social cybersecurity, and strong objectivity.

In chapter 4, the research approach was explained. Design justice and exploratory qualitative research formed the methodology. Semi-structured interviews and thematic analysis were chosen as the methods. Ethical considerations were also laid out.

In chapter 5, the results were shared with the help of the thematic analysis process.

In chapter 6, the results were discussed in light of the research questions and possible solutions to concerns brought up in the results were suggested.

7.1 Key findings

1) **Are queer people of colour especially vulnerable to attacks on their privacy?**

   The results of this thesis suggest that queer people of colour are vulnerable to attacks on their privacy due to their identity, especially so if they are politically active.

2) **Are queer people of colour fully covered by existing privacy regulations and information security measures?**

   The results of this thesis suggest that queer people of colour are not fully covered by existing privacy regulations, especially trans people, who do not receive extra coverage under GDPR due to gender not being classed as 'sensitive'. Information

security measures also seem to lack, such as when a respondent was stalked through a mobile payment app due to there being no blocking function on the app.

3) **Which specific unsafe situations are queer people of colour exposed to through use of technology?**

Interviewees had experienced hacking, harassment, death threats, and rape threats. One interviewee had been forced to change name and address due to someone finding their address online and turning up at home. Multiple interviewees had experienced their families seeing information they didn't want them to see when they were young and not yet open about their gender/sexuality.

4) **Do queer people of colour have specific security concerns?**

The results suggest that queer people of colour had specific security concerns. Every interviewee mentioned far-right extremists as a concern when navigating online, even if they had not had personal experience with far-right harassment. Interviewees were worried about the potential consequences of tech platforms gathering sensitive data about them.

5) **Which alternative strategies do queer people of colour use to stay safe outside already existing digital security frameworks?**

Interviewees used a varied set of tactics to try to maintain digital safety. Informal measures when they were not yet open to their families, such as deleting browser history and using misleading names for folders and bookmarks. As adults, the interviewees restricted content on their social media profiles, didn't use their real names online, and self-censored. They kept their phones close by, changed phone numbers to pre-empt harassment, and left phones behind to prevent location tracking. Interviewees used hidden folders for images and timed disappearing content. During waves of harassment, interviewees would use friends or alternative profiles to stay updated on the situation online and report serious incidents to the police. Interviewees also used coded communication online to alert friends to dangerous situations or confirm their identity. Non-defensive tactics such as intentionally circumventing Facebook's moderation and using anonymous accounts to keep track of far-right extremists were also used.

Interviewees also outlined ways they thought they could be made safer, which included more legislation for social media companies, social media platforms exclusively made for queer people of colour, and non-governmental organisations that work to help with digital safety.

7.2 Future research

There are possible pathways to continuing the research done in this thesis. This is meant to be a non-exhaustive list of suggestions.

Interviewees mentioned multiple times that they would have had to do things differently if they were young today, while research points towards both young LGBT people and young people of colour spending more time online (GLSEN et al., 2013; Rideout et al., 2011). A potential research direction could specifically focus on young queer people of colour and their experiences with modern technology and digital safety.

Another theme that came up multiple times was the differing situations for queer people of colour worldwide, such as the way dating apps can be used to lure queer people into dangerous situations (Carroll, 2019; Noack, 2014). There is potential for future research focusing on queer people of colour and digital safety in countries where being queer is criminalised.

In much of the research done on queer people and technology, such as Vogels (2020), there was only a focus on lesbian, gay, and bisexual people. Future research could look at trans people (other parts of the queer community) specifically.

Another potential continuation from the research done in this thesis could be setting up a digital security clinic in the style of Havron et al. (2019) or Citizen Clinic.

8 References

About EFF. (2007, July 10). Electronic Frontier Foundation. https://www.eff.org/about

Anderson, M., Vogels, E., & Turner, E. (2020). *The Virtues and Downsides of Online Dating*. Pew Research Center. https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2020/02/PI_2020.02.06_online-dating_REPORT.pdf

Ansari, T. (2019, July 1). This Muslim journalist embraced social media until it 'ruined' his life. *First Draft*. https://firstdraftnews.org:443/articles/this-muslim-journalist-embraced-social-media-until-it-ruined-his-life/

Asare, J. G. (2022, February 22). The Evolution Of Whiteness In The United States. *Forbes*. https://www.forbes.com/sites/janicegassam/2022/02/22/the-evolution-of-whiteness-in-the-united-states/

Auchard, E., Stubbs, J., & Prentice, A. (2017, June 27). New computer virus spreads from Ukraine to disrupt world business. *Reuters*. https://www.reuters.com/article/us-cyber-attack-idUSKBN19I1TD

BBC. (2021, February 9). Who are the Uighurs and why is the US accusing China of genocide? *BBC News*. https://www.bbc.com/news/world-asia-china-22278037

Better Business Bureau. (2022, January 25). *BBB Scam Alert: Bored? Think twice before taking that Facebook quiz*. https://bbb.org/article/scams/16992-bbb-scam-alert-bored-think-before-taking-that-facebook-quiz

Blond, S. L., Chua, Z. L., Uritesc, A., Saxena, P., Gilbert, C., & Kirda, E. (2014). A Look at Targeted Attacks Through the Lense of an NGO. *Proceedings of the 23rd USENIX*

Security Symposium, 543–558. https://www.usenix.org/sites/default/files/sec14_full_proceedings.pdf

Brammer, J. P. (2017). Bullying is driving LGBTQ people out of tech, according to new study. *NBC News*. https://www.nbcnews.com/feature/nbc-out/bullying-driving-lgbtq-people-out-tech-study-finds-n752646

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Brooks, S. (2018). *Defending Politically Vulnerable Organizations Online*. Center for Long-Term Cybersecurity. https://cltc.berkeley.edu/wp-content/uploads/2018/07/CLTC_Defending_PVOs.pdf

Brown, T. N. T., & Herman, J. L. (2015). *Intimate Partner Violence and Sexual Abuse Among LGBT People*. The Williams Institute, UCLA School of Law. https://williamsinstitute.law.ucla.edu/wp-content/uploads/IPV-Sexual-Abuse-Among-LGBT-Nov-2015.pdf

Browne, A. J., Varcoe, C. M., Wong, S. T., Smye, V. L., Lavoie, J., Littlejohn, D., Tu, D., Godwin, O., Krause, M., Khan, K. B., Fridkin, A., Rodney, P., O'Neil, J., & Lennox, S. (2012). Closing the health equity gap: Evidence-based strategies for primary health care organizations. *International Journal for Equity in Health*, *11*(1), 59. https://doi.org/10.1186/1475-9276-11-59

Burrough, B., Ellison, S., & Andrews, S. (2014, April 23). The Snowden Saga: A Shadowland of Secrets and Light. *Vanity Fair*. https://www.vanityfair.com/news/politics/2014/05/edward-snowden-politics-interview

Butler, D. (2007). Data sharing threatens privacy. *Nature*, *449*(7163), 644–644. https://doi.org/10.1038/449644a

Caraballo, A. (2022). Remote Learning Accidentally Introduced a New Danger for LGBTQ Students. *Slate*. https://slate.com/technology/2022/02/remote-learning-danger-lgbtq-students.html

Carley, K. M. (2020). Social cybersecurity: An emerging science. *Computational and Mathematical Organization Theory*, *26*(4), 365–381. https://doi.org/10.1007/s10588-020-09322-9

Carroll, O. (2019). In Moscow, gangs are setting up dates with gay men to attack them and steal their money. *The Independent*. https://www.independent.co.uk/news/world/europe/gay-hunters-russia-moscow-apps-gangs-homophobia-a8865376.html

Cartier, M. (2013). *Baby, You Are My Religion: Women, Gay Bars, and Theology Before Stonewall*. Routledge.

Chai, W., & Rosencrance, L. (2021, May). What is a hacker? *SearchSecurity*. https://www.techtarget.com/searchsecurity/definition/hacker

Chen, C., & Dell, N. (2019). Computer Security and Privacy in the Interactions Between Victim Service Providers and Human Trafficking Survivors. *Proceedings of the 28th USENIX Security Symposium*, 89–104. https://www.usenix.org/system/files/sec19-chen-christine.pdf

Citizen Clinic. (n.d.). *CLTC*. Retrieved 5 June 2022, from https://cltc.berkeley.edu/about-us/citizen-clinic/

Columbus, L. (2020, April 5). 2020 Roundup Of Cybersecurity Forecasts And Market Estimates. *Forbes*. https://www.forbes.com/sites/louiscolumbus/2020/04/05/2020-roundup-of-cybersecurity-forecasts-and-market-estimates/

Costanza-Chock, S. (2018). *Design Justice: Towards an Intersectional Feminist Framework for Design Theory and Practice*. Social Science Research Network. https://papers.ssrn.com/abstract=3189696

CNIL. (2020, December 10). *Cookies: Financial penalties of 60 million euros against the company GOOGLE LLC and of 40 million euros against the company GOOGLE IRELAND LIMITED*. https://www.cnil.fr/en/cookies-financial-penalties-60-million-euros-against-company-google-llc-and-40-million-euros-google-ireland

Crenshaw, K. (1989). Demarginalizing the Intersection of Race and Sex: A Black Feminist Critique of Antidiscrimination Doctrine, Feminist Theory and Antiracist Politics. *University of Chicago Legal Forum*, *1989*(1), 139–167.

Dastin, J. (2018). Amazon scraps secret AI recruiting tool that showed bias against women. *Reuters*. https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G

Eggebø, H., Stubberud, E., & Karlstrøm, H. (2018). *Levekår blant skeive med innvandrerbakgrunn i Norge*. https://www.nordlandsforskning.no/nb/publikasjoner/report/levekar-blant-skeive-med-innvandrerbakgrunn-i-norge

Eklöf, N., Abdulkarim, H., Hupli, M., & Leino-Kilpi, H. (2016). Somali asylum seekers' perceptions of privacy in healthcare. *Nursing Ethics*, *23*(5), 535–546. https://doi.org/10.1177/0969733015574927

Ellis, C., Adams, T. E., & Bochner, A. P. (2011). Autoethnography: An Overview. *Historical Social Research*, *36*(4), 273–290. https://www.jstor.org/stable/23032294

Fjeld, I. E. (2020, June 16). Norges Smittestopp-app blant de verste i verden på personvern. *NRK*. https://www.nrk.no/norge/norges-smittestopp-app-blant-de-verste-i-verden-pa-personvern-1.15054311

GLSEN, CiPHR, & CCRC. (2013). *Out Online: The Experiences of LGBT Youth on the Internet*. https://www.glsen.org/sites/default/files/2020-01/Out_Online_Full_Report_2013.pdf

Harding, S. (1995). "Strong objectivity": A response to the new objectivity question. *Synthese*, *104*(3), 331–349. https://doi.org/10.1007/BF01064504

Harrison, S. (2019). Five Years of Tech Diversity Reports—And Little Progress. *Wired*. https://www.wired.com/story/five-years-tech-diversity-reports-little-progress/

Havron, S., Freed, D., Dell, N., Chatterjee, R., McCoy, D., & Ristenpart, T. (2019). Clinical Computer Security for Victims of Intimate Partner Violence. *Proceedings of the 28th USENIX Security Symposium*, 104–122. https://www.usenix.org/system/files/sec19-havron.pdf

Holloway, I., & Galvin, K. (2016). *Qualitative Research in Nursing and Healthcare*. Wiley-Blackwell.

Human Rights Watch. (2014). *"They Know Everything We Do": Telecom and Internet Surveillance in Ethiopia*. Human Rights Watch. https://www.hrw.org/report/2014/03/25/they-know-everything-we-do/telecom-and-internet-surveillance-ethiopia

Human Rights Watch. (2016). *"Tell Me Where I Can Be Safe": The Impact of Nigeria's Same Sex Marriage (Prohibition) Act*. Human Rights Watch. https://www.hrw.org/report/2016/10/20/tell-me-where-i-can-be-safe/impact-nigerias-same-sex-marriage-prohibition-act

Høibråten, A. C. C. (2018). *Dobbel dose annerledes. En kvalitativ studie av unge skeive med etnisk minoritetsbakgrunn i Oslo.* [Master's thesis, University of Oslo]. https://www.duo.uio.no/handle/10852/63414

The Initiative for Equal Rights. (2019). *2019 Human Rights Violations Report Based on Real or Perceived Sexual Orientation or Gender Identity*. https://theinitiativeforequalrights.org/wp-content/uploads/2019/12/2019-Human-Rights-Violations-Reports-Based-on-SOGI.pdf

International Association of Privacy Professionals (IAPP). (n.d.). *What is Privacy*. Retrieved 17 March 2022, from https://iapp.org/about/what-is-privacy/

International Organization for Standardization. (2018). *Information technology – Security techniques – Information security management systems – Overview and vocabulary* (ISO/IEC 27000:2018). https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

Job, C. P. (2022, February 16). It is illegal for LGBTQ+ Nigerians to gather. This app offers a safe opportunity to form community. *Xtra*. https://xtramagazine.com/power/lgbtq-nigerians-qtalk-218245

Kimmerer, R. W. (2015). *Braiding Sweetgrass: Indigenous Wisdom, Scientific Knowledge and the Teachings of Plants*. Milkweed Editions.

Kosinski, M., Stillwell, D., & Graepel, T. (2013). Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences*, *110*(15), 5802-5805. https://doi.org/10.1073/pnas.1218772110

Loh, J., & Walsh, M. J. (2021). Social Media Context Collapse: The Consequential Differences Between Context Collusion Versus Context Collision. *Social Media + Society*, *7*(3), 20563051211041650. https://doi.org/10.1177/20563051211041646

Maxwell, J. A. (2013). *Qualitative Research Design: An Interactive Approach: An Interactive Approach*. SAGE.

Menn, J. (2017, March 29). A scramble at Cisco exposes uncomfortable truths about U.S. cyber defense. *Reuters*. https://www.reuters.com/article/us-usa-cyber-defense-idUSKBN17013U

Morrow, S. L. (2005). Quality and trustworthiness in qualitative research in counseling psychology. *Journal of Counseling Psychology*, *52*(2), 250–260. https://doi.org/10.1037/0022-0167.52.2.250

Moss, R. (2019, September 29). 'My World Is Very Dark Right Now': What It's Like To Be Targeted By Baby Ads After Miscarriage. *HuffPost UK*. https://www.huffingtonpost.co.uk/entry/women-affected-by-miscarriage-and-infertility-are-being-targeted-with-baby-ads-on-facebook_uk_5d7f7c42e4b00d69059bd88a

Munroe, R. (2009). *Security*. Xkcd. https://xkcd.com/538/

Naples, N. A. (2017). Strong Objectivity. In *The Blackwell Encyclopedia of Sociology* (pp. 1–2). John Wiley & Sons, Ltd. https://doi.org/10.1002/9781405165518.wbeoss286.pub2

Noack, R. (2014). Could using gay dating app Grindr get you arrested in Egypt? *Washington Post*. https://www.washingtonpost.com/news/worldviews/wp/2014/09/12/could-using-gay-dating-app-grindr-get-you-arrested-in-egypt/

Qtalk. (n.d.). Retrieved 5 June 2022, from https://play.google.com/store/apps/details?id=com.primedsoft.qtalk

Ravitch, S. M., & Riggan, M. (2012). *Reason & Rigor: How Conceptual Frameworks Guide Research*. SAGE.

GDPR [General Data Protection Regulation]. (2016). *The Official Journal of the European Union*, *59*(L119). https://eur-lex.europa.eu/eli/reg/2016/679/oj

Rideout, V., Lauricella, A., & Wartella, E. (2011). *Children, Media, and Race: Media Use Among White, Black, Hispanic, and Asian American Children*. Northwestern University. https://cmhd.northwestern.edu/wp-content/uploads/2011/06/SOCconfReportSingleFinal-1.pdf

Rigot, A. (2022). *Digital Crime Scenes*. The Berkman Klein Center for Internet & Society at Harvard University. https://cyber.harvard.edu/sites/default/files/2022-03/Digital-Crime-Scenes_Afsaneh-Rigot-2022.pdf

Rivera, L. A. (2012). Hiring as Cultural Matching: The Case of Elite Professional Service Firms. *American Sociological Review*, *77*(6), 999–1022. https://doi.org/10.1177/0003122412463213

Robson, C. (2011). *Real World Research*. Wiley.

Sandelowski, M. (1995). Sample size in qualitative research. *Research in Nursing & Health*, *18*(2), 179–183. https://doi.org/10.1002/nur.4770180211

Savage, R. (2019, November 14). Trans people find fault with Tinder's efforts at inclusion. *Reuters*. https://www.reuters.com/article/us-global-rights-tinder-trfn-idUSKBN1XN2VL

SB-1121 California Consumer Privacy Act of 2018. (2018). *California Legislative Information.* https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121

Schiffer, Z. (2021). Netflix employee at center of Dave Chappelle protest resigns. *NBC News*. https://www.nbcnews.com/tech/tech-news/netflix-employee-center-dave-chappelle-protest-resigns-rcna6362

Scott, A., Kapor Klein, F., & Onovakpuri, U. (2017). *Tech Leavers Study*. The Kapor Center for Social Impact (KCSI). https://www.kaporcenter.org/wp-content/uploads/2017/08/TechLeavers2017.pdf

Shenton, A. K. (2004). Strategies for ensuring trustworthiness in qualitative research projects. *Education for Information*, *22*(2), 63–75. https://doi.org/10.3233/EFI-2004-22201

Shieber, J. (2018, July 23). Tall Poppy aims to make online harassment protection an employee benefit. *TechCrunch*. https://social.techcrunch.com/2018/07/22/tall-poppy-aims-to-make-online-harassment-protection-an-employee-benefit/

Smith, H. J., Dinev, T., & Xu, H. (2011). Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly*, *35*(4), 989–1015. https://doi.org/10.2307/41409970

Statt, N. (2021). Slack's new DM feature can be used to send abuse and harassment with just an invite. *The Verge*. https://www.theverge.com/2021/3/24/22348422/slack-connect-direct-message-abuse-harassment

Tall Poppy—How it Works. (n.d.). Retrieved 5 June 2022, from https://www.tallpoppy.com/how-it-works

Taylor, K., & Silver, L. (2019). *Smartphone Ownership Is Growing Rapidly Around the World, but Not Always Equally*. Pew Research Center. https://www.pewresearch.org/global/wp-content/uploads/sites/2/2019/02/Pew-Research-Center_Global-Technology-Use-2018_2019-02-05.pdf

Thomas, E. (2018, March 12). Tagged, tracked and in danger: How the Rohingya got caught in the UN's risky biometric database. *Wired UK*. https://www.wired.co.uk/article/united-nations-refugees-biometric-database-rohingya-myanmar-bangladesh

Tiku, N. (2019). For Young Female Coders, Internship Interviews Can Be Toxic. *Wired*. https://www.wired.com/story/for-young-female-coders-internship-interviews-can-be-toxic/

Tiku, N. (2021). Google's approach to historically Black schools helps explain why there are few Black engineers in Big Tech. *Washington Post*. https://www.washingtonpost.com/technology/2021/03/04/google-hbcu-recruiting/

Tynes, B. M. (2015, December). Online racial discrimination: A growing problem for adolescents. *American Psychological Association*. https://www.apa.org/science/about/psa/2015/12/online-racial-discrimination

United Nations. (1948). *Universal Declaration of Human Rights*. https://www.un.org/en/about-us/universal-declaration-of-human-rights

van der Velden, M., Gjelsten, B. K., Bergersen, G. R., & Jensen, S. M. (2021). Sustainability Competence in Computer Science Education. *Nordic Journal of STEM Education*, *5*(1), 5. https://doi.org/10.5324/njsteme.v5i1.3953

Vincent, J. (2021, April 13). Google is poisoning its reputation with AI researchers. *The Verge*. https://www.theverge.com/2021/4/13/22370158/google-ai-ethics-timnit-gebru-margaret-mitchell-firing-reputation

Vogels, E. (2021). *The State of Online Harassment*. Pew Research Center. https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2021/01/PI_2021.01.13_Online-Harassment_FINAL-1.pdf

Westeng, K. (2018, September 6). Fikk uønskede meldinger fra eks-kjæresten på Vipps—Nå har Vipps gjennomført viktig endring. *Nettavisen*. https://www.nettavisen.no/12-95-3423533941

Whittaker, Z. (2019, May 12). Two years after WannaCry, a million computers remain at risk. *TechCrunch*. https://techcrunch.com/2019/05/12/wannacry-two-years-on/

Yin, R. K. (2015). *Qualitative Research from Start to Finish*. The Guilford Press.

Appendices

Appendix A - Interview guide

Experiences

1. Do you generally feel safe using digital technology?
2. Are there ways being a QTIBIPoC affects how you use digital technology or how you feel using it?
3. Have you experienced any unsafe situations because of using technology? What happened? (Laptop, mobile phones, social media, hate/threats, being "outed", hacked account, doxed, recognised by someone they didn't want to be recognised by e.g. on dating apps, refused entry to country etc.)
4. Are there differences in how you use technology according to how open you are with gender/sexuality? Does it depend on context (e.g. different levels of openness on different platforms/according to anonymity, pre-/post-coming out)?
5. Do you feel like you can say what you want on social media?
6. Do you feel like you can choose not to be online? (Sometimes necessary to be online because of organisational affiliation or not having local community.) [If for some reason you had to delete all your social media and stuff like that, do you think it would affect your ability to participate in community?]

Concerns

7. Do you have any concerns about using technology/the internet/social media? What are they? [too general, either remove because somewhat covered in other questions, or make more specific]
8. Do you believe that there are ways you or other QTIBIPoC you know can be made unsafe through use of technology? If so, how?
9. Have you ever worried about being doxed (when someone spreads your private information online)?
10. Do you have any concerns about how social media platforms use your information? Are some of them specific to being QTIBIPoC?
11. Have you ever been in a situation where someone else (parent/sibling/other family member/partner/friend) had access to your phone/PC/etc.?
12. If yes, did you have strategies to make sure they wouldn't see things you didn't want to? (deleting messages/apps, changing notification settings so that content isn't visible on home screen etc.)

13. Do you have any worries about travelling and technology?

Strategies

14. Which strategies do you use to stay safe when using technology?
15. Do you have a plan for what you would do if you experience a security/privacy breach?
16. Do you use anonymous accounts? Why?
17. Are there certain things you don't tie your real name to online (e.g. using pseudonym or nickname in interviews or work posted online)? Why?
18. Do you choose (or have you ever chosen) not to use a smart phone? Why?
19. Do you choose not to use specific internet platforms? Or have you chosen to stop using some for periods of time? Why?

Ideas

20. Could you think of any strategies/tools you don't have access to that could make using technology safer for you or other QTIBIPoC?
21. Could you think of any strategies/tools that don't exist that could make using technology safer for you or other QTIBIPoC?

Appendix B – Consent form

Are you interested in taking part in the research project *"QTIBIPoC and Digital Security"*?

QTIBIPoC = Queer, Trans, Intersex, Black, Indigenous, Person of Colour

This is an inquiry about participation in a research project where the main purpose is to investigate QTIBIPoC's habits and concerns around digital security. In this letter we will give you information about the purpose of the project and what your participation will involve.

Purpose of the project

The master's thesis project aims to investigate and collect knowledge around QTIBIPoC's habits and concerns around digital security. Data collected will be used to map challenges and possible strategies around digital safety. This project aims to conduct 5-7 interviews. Results of this thesis might be used to publish scientific articles or other derivative works.

Who is responsible for the research project?

The University of Oslo is the institution responsible for the project.

Why are you being asked to participate?

You have indicated that you fit into the category QTIBIPoC or someone has passed on information about this project to you. Approximately 5 other people will be asked to participate in this project.

What does participation involve for you?

If you choose to take part in the project, participation will involve an interview. Your answers will be saved as a sound recording and physical notes.

The interview includes questions about:

- Your identity.
- Your use of digital technology.
- Strategies you use to stay safe using digital technology.
- Thoughts or concerns you have about digital safety.

Participation is voluntary
Participation in the project is voluntary. If you choose to participate, you can withdraw your consent at any time without giving a reason. All information about you will then be deleted. There will be no negative consequences for you if you choose not to participate or later decide to withdraw.

Your personal privacy – how we will store and use your personal data
We will only use your personal data for the purposes specified in this information letter. We will process your personal data confidentially and in accordance with data privacy legislation.

- Only the student writing the thesis will have access to any data collected.
- Your name and contact details will be replaced with a code in transcribed documents. Names and contact details and respective codes will be password protected and stored separately from recordings and transcripts.
- Recordings will be stored on an encrypted hard drive separate from all other data.
- Recordings will be deleted as soon as a transcript has been made.
- Transcripts will be stored securely on University of Oslo servers.
- All participants will be anonymised. General identification categories can be included in the final thesis, such as age range of informants, general overview of distribution of informants' ethnic/racial backgrounds, general overview of the distribution of sexuality/gender identity of participants, but nothing will be individually identifying. Any quotes included in the published thesis will be anonymised and participants will not be recognisable.

What will happen to your personal data at the end of the research project?

The project is currently scheduled to end in December 2021. Personal data will be deleted at the end of the project.

Your rights
So long as you can be identified in the collected data, you have the right to:

- Access the personal data that is being processed about you
- Request that your personal data is deleted
- Request that incorrect personal data about you is corrected/rectified
- Receive a copy of your personal data, and

- Send a complaint to the Data Protection Officer or The Norwegian Data Protection Authority regarding the processing of your personal data

What gives us the right to process your personal data?
We will process your personal data based on your consent.

Based on an agreement with the University of Oslo, NSD – The Norwegian Centre for Research Data AS has assessed that the processing of personal data in this project is in accordance with data privacy legislation.

Where can I find out more?
If you have questions about the project, or want to exercise your rights, contact:

- The University of Oslo via Lara Okafor (lcokafor@uio.no) or Maja Van der Velden (majava@ifi.uio.no).
- Our Data Protection Officer: Roger Markgraf-Bye (personvernombud@uio.no).
- NSD – The Norwegian Centre for Research Data AS, by email: (personverntjenester@nsd.no) or by telephone: +47 55 58 21 17. Reference number for the project: 540368.

Best regards,

Maja van der Velden	Lara Okafor
Supervisor	*Student*

I have received and understood information about the project "QTIBIPoC and Digital Security" and have been given the opportunity to ask questions. I give consent:

- ☐ to participate in an interview
- ☐ that sound is recorded during the interview
- ☐ that information about gender/sexuality/ethnicity/race is saved until the project ends

I give consent for my personal data to be processed until the end date of the project, approx. Dec 2021.

(NAME in upper case letters) (Signature) (Date)