Security and privacy challenges of using technology in personal, professional, and involuntary relationships

by

Borke Obada-Obieh

B.Sc., Covenant University, 2013

M.Sc., Carleton University, 2017

A THESIS SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF

Doctor of Philosophy

in

THE FACULTY OF GRADUATE AND POSTDOCTORAL STUDIES

(Electrical and Computer Engineering)

The University of British Columbia

(Vancouver)

February 2022

The following individuals certify that they have read, and recommend to the Faculty of Graduate and Postdoctoral Studies for acceptance, the thesis entitled:

Security and privacy challenges of using technology in personal, professional, and involuntary relationships

submitted by **Borke Obada-Obieh** in partial fulfillment of the requirements for the degree of **Doctor of Philosophy** in **Electrical and Computer Engineering**.

Examining Committee:

Konstantin Beznosov, Professor, Electrical and Computer Engineering, UBC
Supervisor

Sidney Fels, Professor, Electrical and Computer Engineering, UBC
Supervisory Committee Member

Leanne Currie, Associate Professor, School of Nursing, UBC
University Examiner

Mohammad Khalad Hasan, Assistant Professor, Computer Science, UBCO
University Examiner

Additional Supervisory Committee Members:

Karthik Pattabiraman, Professor, Electrical and Computer Engineering, UBC
Supervisory Committee Member

Abstract

This dissertation reports on the security and privacy challenges of using technology in personal, professional, and involuntary relationships.

We investigated these challenges by conducting semi-structured interviews and focus groups with participants. To study challenges in personal relationships, we recruited 25 participants who stopped sharing at least one online account in the 12 months preceding the study. We recruited 24 participants working from home in the three weeks preceding the study for challenges related to professional relationships and technology use. To investigate involuntary relationships, we recruited 35 sexual assault survivors, support workers, or both. We analyzed our findings using thematic analysis and grounded theory. Further, to understand technology's various characteristics that facilitate abuse and lead to security and privacy concerns, we conducted a literature review of 224 research papers using involuntary relationships as a case study.

We identified various security, and privacy challenges in using technology in relationships. For instance, in ending the sharing of online accounts, participants reported that angry ex-partners impersonated them and hijacked their accounts. Further, in telecommuting, participants sacrificed their privacy and security to maintain their jobs and professional relationships. Our literature review results also show that technology's inherent characteristics facilitate abuse: covertness, anonymity, evolution, boundlessness, publicness, reproducibility, accessibility, indispensability, malleability, and opaqueness. We find these characteristics facilitate and amplify the identified security and privacy challenges of using technology in relationships.

We discuss the insights from our findings, namely that power imbalance is a

prominent problem in technological use in relationships. We also provide a design rubric that developers can use when developing technologies to predict users' security and privacy challenges and recommendations on how some challenges can be addressed. We are optimistic that the insights derived from our thesis could lead to the design of technological solutions that could address users' security and privacy challenges when using technology in various types of relationships.

Lay Summary

We conducted qualitative research on the security and privacy challenges of the use of technology in personal, professional and involuntary relationships. There has been an increase in the reliance on technology to build and support relationships, and with the COVID-19 pandemic, technology reliance is only expected to increase. To understand users' challenges and why they face these challenges, we employed a qualitative approach. We conducted semi-structured interviews and focus groups and uncovered various pain points from users. We also conducted a literature review of previous research papers to identify technology characteristics that facilitate abuse and enhance the identified security and privacy challenges. We provided a design rubric that developers could use to predict security and privacy challenges in new and existing technological solutions. We discussed how some of the identified challenges could be addressed to protect users' security and privacy.

Preface

This research was a fruitful collaboration between the author of the dissertation and the following people: Yue Huang, Konstantin Beznosov (advisor) from the University of British Columbia, and Lucrezia Spagnolo from Vesta Social Innovation Technologies. It is worth mentioning that the work presented comprises research studies that have been published in peer-reviewed international conferences. In particular, the study presented in Chapters 2, 3, 4, 5, 6, and 7 are partly based on the following publications:

- Borke Obada-Obieh, Yue Huang, & Konstantin Beznosov. (2021, August). Challenges and Threats of Mass Telecommuting: A Qualitative Study of Workers. In Proceedings of the Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021) (pp. 675-694).

- Borke Obada-Obieh, Yue Huang, & Konstantin Beznosov. (2020, April). The Burden of Ending Online Account Sharing. In Proceedings of the CHI Conference on Human Factors in Computing Systems (CHI 2020) (pp. 1-13).

- Borke Obada-Obieh, Lucrezia Spagnolo, & Konstantin Beznosov. (2020, August). Towards Understanding Privacy and Trust in Online Reporting of Sexual Assault. In Proceedings of the Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020) (pp. 145-164).

- Borke Obada-Obieh, Yue Huang, Lucrezia Spagnolo, & Konstantin Beznosov. (2022, May). SoK: The Dual Nature of Technology in Sexual Assault. In Proceedings of the Forty-Third Symposium of the Institute of Electrical and

Electronics Engineers, Security and Privacy (IEEE S&P 2022).

The findings from our research led to invited talks, including a talk presented at Netflix's head office and also at Royal Holloway University, London. Further, the research informed the design of the VESTA technological solution [333].

As the author of the dissertation, I identified the research and conducted over 90% of the user study's design, coding, analysis, writing, and presenting of the results in the first, second, third, and fourth study. I was the lead on all of the user interviews conducted in the first, second and third study. I was involved in implementing more than 95% of the framework presented in the fourth study. For all four studies, Yue Huang participated in the qualitative analysis in order to reduce personal biases. All co-authors were involved in refining the research idea, providing feedback on the study design, brainstorming on the best way to present the results, and proofreading the research papers. All the user studies in the thesis received Behavioural Research Ethics (BREB) approved by UBC under protocols #H20-01219, #H18-03521, and #H19-01984.

Table of Contents

List of Tables

List of Figures

Acknowledgments

They say it takes up a village to raise a child. I think the same goes for getting a PhD too. I wouldn't be getting this degree without the help of many amazing, caring, loving, supporting, and encouraging people that God kept in my life repeatedly. I'm very thankful to you Kosta! I remember when I first met you at USEC. You believed in my dream to do research and change the world in my own little way. And out of millions of people you could have chosen, you offered me the opportunity to be in your lab. Thanks for believing in me and encouraging me. Thanks for always suggesting the next fun activity we could do as a lab. It made my PhD journey special and unforgettable. To the fantastic 4! The 4 lab mates who came for a PhD from 4 different countries like me in September 2017. From China, Iran, Germany/Russia, and Columbia. Thank you, Yue, for all the sleepless nights we spent together trying to meet the next CHI, SOUPS, CCS, or S& P deadlines, getting a rejection, going to food buffets to forget all about school, and then trying all over again. It was all worth it in the end! Masoud and Zhila, thanks for all the conversations and advice you have given me over the years. Artemij, thank you for being so down-to-earth and always helping us be realistic in our expectations. Thanks, Julian, for always reminding us how important family is.

My list of thanks could go on and on. Thanks to the Ayenis for all the support. Thanks, Layo, for all the encouragement and for being a big supporter of my many dreams. Gracehouse has also been very instrumental to this journey for me (Larisa, Alan, Kathy, Sodam, Ife, Sydney, Yeeun, Yeonjoo, Armani, Sarah and Teah). Living with these amazing people in a community in Gracehouse is one of the best things that happened to me during this journey. Thanks for helping me get through my many deadlines and for all your prayers and unending love.

To my one and only Mamalistic! Thanks for loving, always understanding and coping with my ever-busy schedule. Thanks, Sucrolistic and Kesilistic for being the best siblings EVER and for always cheering me on. To Samuel, thanks for loving me through this all and for being EXTREMELY supportive. Always listening and always caring. Thank you.

Above all, I thank God for everything. I thank Him for every failure and rejected papers. Through those, I learned how to be a better researcher. I also thank Him for the successes as well and for helping me to get a PhD degree!

Dedication

To you Dadlistic. I did this for you. Love you today, tomorrow, and forever.
33332907.

Chapter 1

Introduction

The use of technology, especially in building or supporting relationships, has increased dramatically. Over the past two decades, technology has become more widespread and is used in various contexts [194, 251, 305, 337]. For instance, technology is used in health care to detect malicious cancerous cells and reduce the frequency of doctors errors [17, 339], in the armed forces to save lives [297], in transportation systems to increase speed and efficiency [134], by environmentalists to tackle issues of climate changes [203], and in personal lives to improve physical well-being [208]. However, the prominent use of technological solutions is to facilitate the creation of relationships or to support existing ones [82, 96, 194, 289, 334]. This includes the use of social media, dating sites, and professional networking platforms (such as Facebook, Match.com, LinkedIn, Twitter, Instagram) to build personal and professional relationships [50, 310]. It also includes the sharing of online accounts (such as Netflix or online bank account) as a sign of trust and intimacy to support existing relationships [166, 244, 302].

The COVID-19 pandemic has led to heavier reliance on technology. With many lock-downs still in place and social distancing in effect, there has been a surge in using technology to facilitate communication and support relationships [242]. In situations where face-to-face communication would have been necessary, now more than ever, people are more dependent on technology to bridge the gap in communication and in building and maintaining relationships. For instance, there is an increase in using telecommuting technologies to foster communication and

relationships with co-workers and their organizations [68] as well as classroom technologies for students [178]. The strong reliance on technology is expected to increase as the world settles into this *new normal* [224, 240].

With the rise in technology reliance comes a rise in security and privacy concerns. For instance, there is an increase in online security fraud for users of technological solutions [242]. Understanding and addressing the specific security and privacy challenges that users encounter in technology usage in relationships is important. Using technologies in online and offline relationships could often come with severe outcomes when the relationship do not go as planned (for example, severe outcomes could include cyber-bullying, stalking, online and offline sexual harassment, and in some severe cases, death) [66, 102, 177, 233]. This dissertation aims to understand the security and privacy challenges that users encounter in using technologies in various types of relationships and potentially how those challenges can be addressed.

For clarity, we define technology broadly as a collection of systems "that allow users to exchange digital information over networks" [32]. In this dissertation, we use technology as an umbrella term for all types of mobile, web-based, and internet-enabled services, platforms, solutions, and devices. We define relationship using Hamilton's [127] description. The author defines human relations as the "ability to interact effectively with diverse others in a variety of situations" [127]. Relationships can broadly be classified into two categories, personal and professional relationships [321]. Examples of personal relationships include family, friends, acquaintances, and romantic partners. An example of professional relationships in the work context include interactions between employees and the employer. Both personal and professional relationships can either be voluntary or non-voluntary [321]. Voluntary relationships refer to relationships were both parties willingly decided to be in the relationship. The opposite is involuntary where both parties are forcefully in the relationship. For our dissertation, we focused on case studies for personal & voluntary, professional & non-voluntary, and personal & non-voluntary relationships. Table 1.1 shows our research focus. For simplicity, we refer to personal & voluntary as *personal relationships*, professional & non-voluntary as *professional relationships*, and personal & non-voluntary as

	Personal Relationships	Professional Relationships
Voluntary	X	X
Non-voluntary	X	-

Table 1.1: The X represents areas that we investigated.

involuntary relationships.

In this dissertation, we present the security and privacy challenges that people encounter in:

1. Personal relationships and technology use: Here, we studied people's security and privacy challenges when they stop sharing online accounts in personal relationships.

2. Professional relationships and technology use: Here, we studied employees' security and privacy challenges while telecommuting with co-workers and their bosses but not involuntarily.

3. Involuntary relationships: Here, we studied security and privacy challenges that sexual assault survivors encounter in using technology to report their perpetrators to the police. In this complex scenario, survivors face a dilemma whereby they want to use technology to report the sexual assault incident, but this is complicated because of their previous unwanted relationship and contact with the perpetrator. Beside personal and professional relationships, we studied involuntary relationships to understand the security and privacy issues that could arise in this context and how we could address them.

To address the identified security and privacy challenges, we developed design rubrics that technologists could consider when developing technological solutions for people in personal, professional, or involuntary types of relationships.

1.1 Problem Overview

1.1.1 Personal Relationship: Why study challenges with ending the sharing of online accounts?

Sharing online accounts has become a prevalent practice among social groups and individuals. In the US alone, 54% of Americans share accounts, with 41% sharing online shopping accounts (e.g., Amazon Prime), and 75% sharing streaming accounts (e.g., Netflix, Hulu) [49, 163]. A recent discussion via Twitter among the members of the UK's Parliament shows sharing accounts is a common practice [160], even when a high level of information security is expected [230, 246].

However, privacy and security challenges arise when account sharing ends, especially when the account was never designed to be shared in the first place. Online accounts are not always designed to effectively facilitate the ending of sharing between users [70, 166, 218]. While previous work focuses on why people share accounts [201, 244] and how they begin the sharing process [166, 201], no study has investigated the factors that complicate the ending of account sharing in personal relationships.

1.1.2 Professional Relationship: Why study challenges with mass telecommuting?

Our investigation into telecommuting challenges is a response to a clear need for safer work-from-home practices as the rise in telecommuting has led to an increase in cyber-attacks [22, 165, 191, 229].

The global COVID-19 pandemic has resulted in the world's largest telecommuting situation [14]. In 2018, the U.S. Bureau of Labor Statistics report showed that only 8% of all employees work from home at least one day of the week, while 2% worked fully from home [23, 232]. However, most employees now work from home. Recent research from Stanford indicates that as of June 2020, 42% of the labor force was telecommuting (with 33% unemployed and 26% working in essential services) [24, 351]. Researchers estimate employers plan to keep 20% of their workers working from home after the pandemic ends, mainly to reduce costs [212]. Another recent survey shows that 47% of the respondents aim

for their workers to telecommute full-time [120]. Further, some major tech companies have already switched to either long-term or permanent work-from-home model [48, 61, 172, 271].

With a remote workforce and everyone working digitally, the threat landscape increases. Research shows that 91% of respondents experienced an increase in cyber-attacks because of employees telecommuting [22]. Further, the Canadian Press reported a 1,350% increase in cloud-related attacks and a 4,000% increase in ransomware emails [211]. Remote working can also be problematic when employees' personal computers are not updated with the most recent security protocols and software. Employees risk exposing the entire system to various types of cyber-attacks and compromising their professional relationships. Major organizations have suffered data breaches targeted at employees. For instance, the World Health Organization reported a fivefold increase in cyber-attacks, with the most recent attack targeting their employees [346]. There has been a spike in phishing attacks in Italy because of people teleworking [173]. In addition, the threat model in a home environment differs from that seen in the physical office workplace. For instance, some company devices used in teleworking are linked to home or less secure Wi-Fi networks. These company devices may not have the physical security provided in the workplace.

To address the security and privacy concerns of working from home, research is needed to understand the specific challenges and threats that employees experience while telecommuting. Several telecommuting research projects compared workers' productivity while working from home and in physical office locations [4, 7, 25, 57, 294]. Some research on working from home also provides tips and strategies for securing the home internet network for employees while telecommuting [93, 179, 226]. However, to the best of our knowledge, no research has focused on employees' security and privacy concerns regarding telecommuting with their co-workers.

1.1.3 Involuntary Relationship: Why study challenges with reporting sexual assault using technological solutions?

Our investigation into designing safe spaces online for anonymous third-party reporting (TPR) is a response to the clear need for a confidential and accessible plat-

form that survivors of sexual assault can use to communicate their experiences hoping to hold perpetrators accountable.

The stark reality is that 1 in 3 Canadian women will experience sexual assault in their adult life [236]. Further, 1 in 14 American men and 1 in 5 American women have been victims of completed or attempted sexual assault during their lifetime [306].

Sexual assault has no single impact but affects multiple areas of the survivor's life, including but not limited to the survivor's somatic and psychological health [55, 73]. One in four survivors reported they had difficulty carrying out everyday activities because of the incident [193]. Further, one in six survivors reported experiencing three or more longer-term emotional consequences, such as post-traumatic stress disorder, substance abuse, depression, and suicidal thoughts [75, 190, 193].

However, statistics alone fail to capture the significant repercussions of sexual assault on survivors, not only because the effects of such trauma are unquantifiable [55] but also because sexual assault is greatly underreported [231, 278]. Only 5% of cases are reported to the police [249], and only 11% of those reported cases eventually lead to the conviction of the perpetrator [285].

1.2 Goal and Methodology

Our dissertation aims to contribute to the body of knowledge on the security and privacy challenges of using technological solutions in relationships. Based on our findings, we discuss design suggestions, guidelines, and rubrics for designing technologies in this context.

We conducted interviews and focus groups with participants to investigate their security and privacy challenges. Our results showed a major theme across the three scenarios: the possibility of power imbalance in using technology in relationships. Further, the potential of misuse and abuse of technology by the person with the greater power (in terms of technology use) in the relationship. To mitigate this problem, we carried further research to uncover technology's inherent characteristics that facilitate abuse. Using the involuntary relationship as a case study, we conducted a literature review of 224 papers that discusses the use of technology to facilitate, report, or prevent sexual assault. Through this review, we discovered

ten inherent characteristics of technology that facilitate abuse. We present these characteristics as guidelines for technologists regarding possible ways others can misuse their technological solution in relationships, resulting in security and privacy challenges for users.

1.3 Research Summary

1.3.1 Security and privacy challenges of ending online account sharing

In the first study, we investigated the security and privacy challenges that complicate the ending of online account sharing in various types of personal relationships by asking:

- RQ1: What are the security and privacy challenges people encounter in ending sharing of online accounts?

We addressed our research questions by conducting semi-structured interviews ($N = 25$) with participants who had shared at least one account in the 12 months preceding the study. Participants had various types of personal relationships with those with whom they shared accounts. The interviews focused on the accounts, why and how the sharing began and ended, and what made the process difficult. We analyzed data using thematic analysis [126].

Finding 1: *We discovered reasonable but unsupported sharing use cases for some accounts that are not designed for sharing.* Participants were torn between attempting to satisfy their appropriate need for sharing and maintaining their security and privacy.

Finding 2: *Participants' privacy and security were more at risk when they stopped sharing accounts that were never designed for sharing.* We offer specific recommendations for designing these accounts to allow sharing between users without sharing account passwords.

1.3.2 Security and privacy challenges of mass telecommuting

The aim of our second study was to answer the following research question:

- RQ 2: What are employees' security and privacy challenges, threats, and perceived risks when working from home?

We addressed our research question by conducting semi-structured interviews with 24 participants. Participants were employees who had been working from home in the three weeks preceding the study. We asked questions related to their challenges with telecommuting and analyzed the results using thematic analysis.

Finding 3: *We discovered concerns that need to be addressed to protect the security and privacy of employees and employers while telecommuting.* Participants were also torn between maintaining their professional relationship and protecting their security and privacy. We identified the perceived outcomes of threats associated with these concerns. We grouped our findings into four categories of challenges and threats: technological, human, organizational, and environmental. We further grouped our findings into the identified outcomes of threats to security and privacy and created threat models that emerged from our results.

1.3.3 Security and privacy challenges with using technological solutions to report sexual assault

The objective of the third study is to answer these research questions:

- RQ3: What are survivors' privacy and security concerns (if any) regarding trusting an online reporting system?
- RQ4: What could help participants trust an online reporting system?

We addressed our research questions by conducting six focus groups and eight individual semi-structured interviews with 35 participants. They were survivors, sexual assault support workers, or both. We asked questions relating to participants' concerns with trusting an online system for reporting sexual assault and analyzed the results using thematic analysis.

Finding 4 (under RQ 3): *We group our findings into technological and emotional concerns, and we show how technological concerns can lead to emotional issues for survivors.* For example, the technological concern about the *insecurity of technology* can lead to the emotional issue of *anxiety* about making an online

report, the *fear of perpetrators having access to the sexual assault report*, and the *re-victimization of survivors.*

Finding 5 (under RQ4): *We discovered concerns that technologists need to consider in developing technological solutions for survivors.* For instance, on the one hand, survivors did not trust that a technological solution could protect their anonymity and privacy from both the perpetrators and the police. On the other hand, the police did not trust that the anonymous reports sent from a technological solution were linked to real survivors. Therefore, technologists need to find a balance in how technology can ensure both parties trust the system.

1.3.4 The characteristics of technology that facilitate abuse

A major theme emerged from the three previous studies: power imbalance in using technology in relationships and the potential abuse of technology by the person in the relationship with the greater technological power. To mitigate this problem, we carried further research to uncover technology's inherent characteristics that facilitate abuse. The objective of the research was to answer this research question:

- RQ5: What characteristics of technology facilitates abuse?

We addressed our research questions by conducting a literature review of 224 research papers—the papers discussed how technology facilitates the abuse of victims. We analyzed the papers using grounded theory.

Finding 6: *We identified ten characteristics of technology that facilitate abuse.* These characteristics are covertness, anonymity, evolution, boundlessness, reproducibility, accessibility, publicness, indispensability, malleability, and opaqueness. We show how these attributes facilitate the abuse of victims in other types of relationships.

1.4 Contributions

In summary, we make three main contributions to the research community:

Contribution 1: We provide insights into the security and privacy challenges of using technology in personal, professional, and involuntary relationships and the

effect of those challenges (e.g., power imbalance). We also offer specific suggestions that could address the identified challenges.

Contribution 2: We identified ten characteristics of technology that enhance these challenges and facilitate the abuse of technology.

Contribution 3: Based on these characteristics, we derive the dimensions of technology and provide a design rubric for technologists for the design and development of solutions that address users' security and privacy challenges in relationships.

Chapter 2

Security and Privacy Challenges of Ending Online Account Sharing

Privacy and security issues arise when account sharing ends, especially when the account was never designed to be shared in the first place. Online accounts are not always designed to effectively facilitate the ending of sharing between users [70, 166, 218]. While previous work focuses on why people share accounts [201, 244] and how they begin the sharing process [166, 201], we investigated the factors that complicate the ending of online account sharing in various types of personal relationships by asking:

- RQ1: What are the security and privacy challenges people encounter in ending sharing of online accounts?

Answering this question can provide insight into how accounts can be designed to better support users in ending account sharing, thereby improving the user experience and safeguarding users' personal information.

For the sake of clarity, we grouped online accounts into the following categories:

Accounts designed for sharing (DS) are accounts that offer multi-user member-

ship plans. Examples include Netflix, Amazon Household, and Spotify Premium Family accounts. Although these services also provide single-user plans, we will use "DS accounts" or "multi-user accounts" to only refer to the multi-user plans.

Accounts not designed for sharing (NDS) are accounts that are intended for only one user. Examples include WhatsApp, Facebook, Instagram, and LinkedIn accounts. We also include the single-user versions of DS accounts in this category. We'll use "NDS accounts" or "single-user accounts" to refer to such accounts.

We defined relationships in the previous chapter. Examples of personal relationships include friendship, family, or romantic relationships.

Key contributions of this chapter are:

- First, we discover *reasonable* but unsupported sharing use cases for some NDS accounts. Participants were torn between attempting to satisfy their appropriate need for sharing and maintaining their security and privacy. Our results suggest that companies offering such NDS accounts should consider supporting these use cases.

- Second is the finding that participants' privacy and security were more at risk when they stopped sharing NDS accounts because the accounts were never designed for sharing. As part of this contribution, we offer specific recommendations for designing these accounts to allow sharing between users without users having to share account passwords.

- Third, we identify negative impacts of ending the sharing of DS and NDS accounts on users, and group them into *cognitive* and *psychosocial* impacts.

  Examples of cognitive impacts are remembering the people with whom accounts were shared, changing passwords, and remembering the accounts across which participants reused passwords.

  Examples of psychosocial impacts are the uncertainty about whether the sharing ended successfully, the frustration of losing personal content, and

the fear of the account being hijacked by the secondary user. Identifying these challenges is important for reducing the cognitive and psychosocial burden of ending account sharing and reducing corresponding security and privacy risks.

We suggest recommendations (and discuss their benefits) for improving the design of online accounts to address the identified challenges.

Our contributions provide insight into the burden of ending online account sharing and add new considerations to the many that already exist when considering account privacy and security.

2.1 Related Work

2.1.1 Account sharing

Several studies have focused on account sharing and the reasons behind it. Egelman et al. [90] conducted a survey of households that made use of the Windows operating system on their home computers. The study aimed to find out whether participants shared single-user accounts on their computers and how sharing occurred. The result of the study was a recommendation to provide family accounts on home computers to aid in account sharing. A more recent study by Matthews et al. [201] investigated why people share accounts and household devices. Using an inventory survey and a 21-day diary study, the authors discovered 6 types of sharing that are related to the reasons people share accounts: borrowing, mutual use, setup purposes, helping other users, broadcasting, and accidental.

Sharing accounts in the context of romantic relationships has received special attention from the academic community. Singh et al. [302] were among the first to study why couples share accounts. The authors carried out open-ended interviews, group interviews, and focus groups during three months with married and de facto couples. They found that people share accounts as a sign of trust, as a key to survival, and because they had no option (e.g., couples with disabilities). More recently, Jacobs et al. [166] conducted interviews and an 8-day diary study that confirmed the results of previous studies and identified additional reasons for

account sharing in romantic relationships, which were the maintenance of the relationship, and to promote intimacy. The aim of another recent study by Park et al. [244] was to understand the account sharing behaviors of people in romantic relationships. Through a survey on Amazon Mechanical Turk, the authors found that couples share accounts to meet goals such as convenience, household maintenance, trust, and relationship maintenance. However, some participants were actively hiding the existence of certain accounts from their partners. Park et al. also suggested design recommendations for better supporting three relationship stages: the start, maintenance, and the end.

Studies of technology in the context of intimate partner abuse (IPA) have described common situations in which abusers coercively access survivors' accounts, and survivors attempt to end this coercive access [109, 112, 202]. Even though some of the account mechanics described in our study with general users may overlap with this prior work, IPA situations are different in that they involve coercive account access and different (potentially severe) consequences for survivors. Multiple studies of how technology affects IPA [109, 112, 202] have described how abusers leveraged coercive control of survivors' accounts and shared household accounts to abuse survivors. For example, an abuser may use coercive access to a survivor's accounts to reset passwords and lock the survivor out, to impersonate the survivor to damage their reputation and relationships, or to surveil the survivor. It should be noted that our study does not explore account ending in the context of abusive situations.

Our research builds on prior work. We expand the scope of investigation with general users by studying the end of account sharing in the context of a variety of personal relationship types, such as friendship, school, and acquaintanceship. We also explore how technology supports this process and what can be done to improve support.

2.1.2 Ending account sharing

Several studies focused on how digital possessions are managed after breakups. Quan-Haase et al. [267] studied the coping strategies employed by young adults (10 unmarried participants) on Facebook after a romantic breakup. The results indicate

that participants remained digitally entangled. For example, because Facebook shows interactions between friends and non-friends, it was possible for participants to continue to learn about their ex-partners' activities, even though they no longer wanted such information. Sas et al., [292] studied how users keep or dispose of their digital possessions after a romantic breakup. The authors conducted semi-structured interviews with 24 students and identified three roles that people take in disposing of their digital possessions: deleters, keepers, and selective disposers.

Researchers from the University of Dundee also studied how users manage their digital possessions after a romantic breakup, with the goal of informing the design of systems aimed at helping people disentangle digitally [155, 218]. The digital possessions studied included videos, chat logs, login details, shared accounts, social media posts, and text messages. The study was carried out with 13 participants. The authors found that after the romantic relationship ended, the role of digital possessions changed, as the possessions now acted as a proof that the relationship existed and was over. Participants managed their digital possessions by hiding, deleting, or abandoning their possessions, and in some cases, letting the possessions fall into disuse.

Our study differs from prior research in two major ways. First, we focus on the end of online shared accounts and we consider different age groups and types of personal relationships. While Sas et al. [292] studied what users do with their digital possessions, we go further to identify the specific security and privacy challenges that users face when managing one type of digital possession — an online shared account. No previous studies have focused their investigation on these challenges. Second, we discuss how systems can be designed to support users during the ending of the sharing of accounts while considering users' security and privacy issues.

2.2 Methodology

2.2.1 Data collection

We recruited participants by advertising on Facebook and on UBC's paid participants study list. Potential participants filled out an eligibility survey. To be eligible

to take part in the study, participants had to be 19 years old or above. Participants had to have stopped sharing at least one account within the last 12 months or be in the process of ending the sharing of an account. We chose to recruit people who were also in the process of ending account sharing to understand any current challenges they might be facing.

We piloted our study procedure with two participants. In the first pilot study, we asked the participant what account she had stopped sharing. We realized that the participant had difficulties remembering most of the accounts she ended sharing. The participant remembered some shared accounts only when the researcher gave examples of commonly shared accounts. Based on this result, we decided to present participants with a list of accounts grouped and categorized by Park et al. [244], to help participants remember their shared accounts. We piloted this approach with a second participant, and we discovered that the participant remembered previously shared accounts easily. We therefore decided to use this approach for the main study. Apart from this change, all other procedures in the pilot interviews were the same as those used in the main study.

After adjusting the study procedure based on the outcomes of the pilots, we recruited participants for the main study. We carried out semi-structured individual interviews with all recruited participants to allow participants to express their thoughts in their own way and add information as they saw fit, without the restriction of a structured interview [65]. We conducted in-person or video interviews based on the participant's preference. In-person interviews were conducted in a quiet meeting room on UBC campus, while video calls were conducted via Skype. Participants interviewed in person were compensated with CAD $20, sent via e-transfer to those participants whom we interviewed via video call. We conducted 11 interview sessions via Skype video, with the rest (14) in person. Data collection was done from December 2018 to February 2019. The research was approved by the UBC Behavioural Research Ethics Board (ID: H18-03521) before any data collection took place.

2.2.2 Interview procedure

We proceeded with the interviews after participants gave informed consent to participate in the study. During each interview, we explained the meaning of shared accounts, giving examples of such accounts. We avoided priming the participants by stating that shared accounts were simply accounts used by the participants and other users. Participants were told that the aim of the study was to understand their experiences using shared accounts.

Participants were then asked to identify the accounts they were sharing or had shared with someone. To help participants remember their shared accounts, we presented them with a list of accounts grouped and categorized by Park et al. [244]. This list itemized most online shared accounts at the time, but we explained to participants that the account list was only a guide. As they identified other accounts that did not appear on the list, they were free to tell us about them (and some did).

After participants identified their shared accounts, we asked them which accounts they were currently sharing and which ones they had stopped sharing. Then we asked participants to give more information about the accounts that they had stopped sharing. We also asked questions about the use of passwords on their accounts. Afterward, we asked for demographic information and compensated the participants. One or two researchers took part in each interview session. All interview sessions were audio recorded.

2.2.3 Data analysis

Two researchers transcribed and coded more than 16 hours of recorded interview sessions, each an average of 40 minutes long. Interviews were analyzed using thematic analysis [126], a "set of procedures designed to identify and examine themes from textual data in a way that is transparent and credible [125]." We followed the data analysis steps outlined by Guest et al. [125]. Two researchers segmented and coded the transcribed interviews into categories, types, and relationships to develop the codebook. Afterward, the researchers identified the themes that emerged from the data. We conducted data analysis concurrently with the collection and reached theoretical saturation after 23 interviews, as no new codes emerged from the last two data collection sessions. Our supplementary material (Appendix [**?**] includes

a saturation graph depicting the total number of codes after each interview.

To calculate inter-coder reliability, we used the percentage agreement metric described by Graham, Milanowski, and Miller [121]. The calculated agreement was above 90%, which indicates high agreement. In addition, three researchers engaged in a code and theme sorting exercise to come to a consensus on the identified themes.

2.2.4 Participants

We recruited 25 participants (16 women and 9 men), aged 19 to 45 years (the mean and median were 27). Table 2.1 provides the detailed demographics of the participants. All participants had stopped sharing at least one previously shared account.

2.3 Results

Our results suggest that negative impacts accompany the ending of account sharing, and we group them into two categories: cognitive and psychosocial. We define cognitive burden as the mental effort involved in ending account sharing and psychosocial burden as the emotional and social cost of ending account sharing. Although we divided these negative impacts into these two categories, it should be noted that cognitive and psychosocial burdens are linked together. All cognitive burdens come with an indirect psychosocial cost, and they often tax users in the form of frustration. We discuss these categories of burden below.

In the rest of the chapter, we refer to each participant using the suffixes "P,""S," and "J" along with their ID, to indicate whether the participant was a primary, secondary, or joint user of the shared account. A primary user is the owner of the shared account. A secondary user is not an owner of the account, but shares it with the primary user. *Joint* users both own the shared account with the intent to have equal rights and privileges.

Cognitive burden

Remembering secondary users. Our participants found it challenging to remember the people with whom specific accounts were shared. Sometimes participants

ID	Age	Gender	Educational Level	Occupation	Ended Sharing	Ended Sharing With
P1	21	W	Bachelor's (Ongoing)	Student	Netflix (s)	Friends
P2	32	M	Master's	Teacher in High School	Netflix (p)	Ex-girlfriend
					Telus (p)	Father
					LinkedIn (p)	Friends
					LinkedIn (p)	Professionals
					Skype (p)	Friends
					Gmail (p)	Friends
P3	45	M	Master's	Information Technology	Amazon (j)	Partner
					Fantasy League Game (p)	Colleague
P4	27	M	Master's (Ongoing)	Master's Student	Netflix (p)	Friend
					Netflix (p)	Wife
P5	25	M	Bachelor's	Finance Clerk	Email Account (p)	Employer
					Bank Account (s)	Father
					Amazon (p)	Mother
P6	28	M	Diploma	Circus Artist Instructor	Bank Account (s)	Parents
					Online Calendar (s)	Colleague
P7	31	M	Master's	Research Assistant	Amazon (p)	Wife
					Amazon (s)	Friend
P8	23	W	Bachelor's	Tutor	Netflix (s)	Boyfriend
					OkCupid (p)	Ex-boyfriend
P9	29	W	Bachelor's	Administrative Assistant	Netflix (s)	Boyfriend
					Apple (p)	Family
P10	29	W	Bachelor's	Tutor	Amazon (s)	Father
P11	29	W	Master's	PhD Student	WeChat (s)	Sister
					Gmail (s)	Sister
					Sephora (p)	Friend
					Game Account (p)	Friend
					Apple (p)	Family
					Baidu (p)	Sister
P12	30	W	Master's	Human Resource Specialist	Bank Account (p)	Parents
					Netflix (p)	Parents
					Gmail (p)	Ex-boyfriend
					Facebook (p)	Friend
P13	27	W	Bachelor's	Unemployed	League of Legends (p)	Brother
					League of Legends (p)	Ex-boyfriend
					Netflix (p)	Brother
					Booking.com (p)	Friend
P14	20	W	Bachelor's	Student	Amazon (p)	Brother
					Facebook (p)	Ex-boyfriend
					Gmail (p)	Classmates
					Craigslist (s)	Roommates
					Netflix (s)	Family
					Soundcloud (s)	Ex-boyfriend
					Xbox (s)	Brother
					Dropbox (s)	Friends
P15	22	M	Bachelor's (Ongoing)	Student	Bank Account (s)	Parents
					iTunes (p)	Father
					Spotify (p)	Sister
					Dropbox (s)	Colleagues
P16	24	M	Bachelor's	General Manager	Bank Account (p)	Ex-girlfriend
					Facebook (p)	Ex-girlfriend
					Yahoo (p)	Ex-girlfriend
					Gmail (p)	Friend
P17	23	W	Bachelor's	Admin in Insurance	Netflix (s)	Boyfriend
					New York Times (p)	Friend
					Bank Account (p)	Parents
P18	25	W	Bachelor's	Respiratory Therapist	Bank Account (s)	Mother
					Nextopia (p)	Friend
					Facebook (s)	Friend
					Instagram (s)	Friend
					Netflix (s)	Friend
P19	21	W	Bachelor's (Ongoing)	Student	Bank Account (p)	Brother
					Netflix (p)	Friend
P20	19	W	Bachelor's (Ongoing)	Student	Bank Account (s)	Mother
					Tumblr (p)	Ex-boyfriend
					Snapchat (p)	Ex-boyfriend
					Amazon (s)	Ex-boyfriend's Friend
					Netflix (s)	Ex-boyfriend
					Uber Eats (s)	Ex-boyfriend
					Office365 (p)	Ex-boyfriend
P21	36	W	Bachelor's	Office Admin	Netflix (s)	Husband
P22	20	W	Bachelor's	Student and Sales Personnel	Google Drive (s)	Ex-boyfriend
P23	32	W	Bachelor's	Secretary	Facebook (p)	Friend
P24	42	M	Master's	Model and Writer	Netflix (p)	Ex-partner
					Bank Account (p)	Ex-partner
					iTunes (p)	Sister
P25	23	W	College (Ongoing)	Student and Part-Time in Insurance	Netflix (s)	Boyfriend
					Bank Account (s)	Mother

Table 2.1: Detailed demographics of participants. P, S, and J represent primary, secondary, and joint users respectively.

forgot that they shared a particular account. As a result, they forgot to end the sharing of that account, even after the sharing was no longer desired. For example, it was during our interview that P20-P remembered that, apart from her mother, she still shared her Microsoft Office 365 account with her ex-boyfriend: *"Oh my gosh. I still share [my Microsoft 365 account] with my ex!"* She didn't want to continue sharing the account; however, she had forgotten that the account was still shared. Similarly, P22-S, who tagged herself as a "self-imposed" secondary user, also described a scenario where the primary user forgot to log out: *"... it was [during] a movie night [with people from a school club] and I was the one who brought the laptop but I don't have [a] Netflix account. So [an acquaintance] logged in with my laptop and then she forgot to sign out, so I've been taking advantage of [the account] [laughs]."* P22-S has been using the Netflix account for about 18 months.

Changing passwords. Password changes were described as both useful to end account sharing, but also problematic in the cognitive burden they introduced. P20-S described the value of password changes in a story about her boyfriend's Netflix account that was shared with multiple people: *"At least 9 people [used his Netflix account] because there were about 5 profiles and then I think each of them has their own people they were sharing it with. [My boyfriend at the time] had to change his password a lot because there were too many people logged in at [once] ... Whoever he shared it with shared it with other people. So if he wants to watch [Netflix] he couldn't, because there were too many people on it, so he would change his password. [That] would log everyone out and then he would be able to watch it and then [he would] share the password and just repeat that cycle."*

When sharing ends, changing passwords can be a tedious process. P2-P, for example, shared his LinkedIn account multiple times with his friends and paid professionals because he needed help in making his account look professional. However, every time he shared his LinkedIn account, he had to change his password after his friends (or professionals) finished editing his account content. P2-P commented on the burden of having to change his passwords multiple times: *"... it's annoying [to change passwords] because I do forget [the new password] ... I've had that problem a few times before where I've lost track of my passwords and answered some [security] questions [or] ... go through the security feature where they email me [on some other platform] just to verify that it is me."*

To avoid the cognitive burden of changing passwords, sometimes participants would request that the secondary user(s) stop logging into the account. P8 illustrated this while describing an incident between her boyfriend (secondary user) and his ex-girlfriend (primary user): *"I happened to be calling [my boyfriend, and he said] ... 'I just got a text from my ex saying, "Can you log out of the Netflix account?"' [My boyfriend's ex] was also sharing [her Netflix account] with other people. So instead of [changing the password for everyone] ... it's easier to just kick one person out."* In this case, changing the password for multiple users who were sharing a Netflix account would have proved even more challenging. This coping mechanism is, however, linked to the burden of remembering secondary users. For this strategy to be carried out effectively, primary users have to remember that a particular secondary user still has access to the account.

Remembering which passwords are reused on which accounts. Participants found it challenging to remember the accounts across which they had reused passwords. P13-P, for instance, used the same password on her game, bank, Netflix, and university student accounts. She had shared her game account with her boyfriend but changed the password when she had a disagreement with him. However, she had forgotten that she used the same password on the other accounts. P13-P only realized this during the interview and noted that she would change the passwords for the other accounts as well.

Some participants coped with the challenge of remembering many passwords by reusing them across shared and non-shared accounts. P16's example illustrates this behaviour: *"[I know reusing passwords] is wrong, but I do [reuse passwords] because it's easier to remember ... I know you should have different passwords for different accounts, but I'm just too lazy ... because I might forget them."* P22 explains further: *"I tend to use the same password for a lot of websites, and just because I told my password to someone for one website means the person basically knows a lot of passwords for many websites."* Previous research [171, 345] also shows that people reuse passwords to avoid remembering multiple passwords.

To lighten the cognitive burden of remembering many passwords, participants sometimes also derived similar passwords. Passwords used on shared accounts were similar or the same to those used on non-shared accounts. P23, who used similar passwords on shared accounts, explained how she modified her password

across accounts: *"I have just one password but then ... I tweak the password a little differently for all of the accounts. Maybe I add an exclamation mark to one, [then] add a number ... ."* Similar passwords are, however, easy to guess. Zhang et al. [357] discovered that if an attacker has access to a password, they can correctly guess the future passwords in 41% of accounts in an offline attack under 3 seconds, and 17% of accounts in an online attack.

Psychosocial burden

The uncertainty of whether the sharing was successfully stopped. Participants were not always sure that changing password was enough to end sharing. Modern devices are kept logged into online services for extended periods of time without re-authentication (thanks to access tokens in OAuth [228] and similar authentication technologies). While this feature is very convenient in single-user scenarios, it leaves primary users uncertain whether and when changing password "kicks out" secondary users. It was particularly problematic when primary users were unwilling to ask the secondary users to stop using the account. For instance, P20-P no longer talked to her ex-boyfriend after their romantic breakup. During the relationship, she shared her private blog hosted on Tumblr [1] with him. When asked if she was still sharing the account, P20-P remarked: *"... I don't know ... I changed my password, and I hoped that it would log him out ... I think the [Tumblr] app is still [on his phone], but I hope he's logged out."*

The annoyance of being unable to migrate content to a new account. Transferring previously shared content to a new account sometimes proved difficult. P15-S, who had shared his father's Apple ID account, explained the challenges he experienced when sharing ended: *"[On migrating the free apps] I would have preferred to be able to transfer [the free apps] automatically [to the new account] because ... that way I [don't] have to manually re-download all the free apps [from] the app store ... It would be nice to save time."* Similarly, participants discussed lost Netflix profiles and the corresponding movie lists recommendations when sharing ended. P4-P commented: *"I used to share my [Netflix] account with other group of people ... Having that account established and then switching over*

[1] https://www.tumblr.com

to another [Netflix] account [to be shared with a new group of people], [it] was difficult to manage all the [profile] list that I create[d]. [I had to] re-establish my entire profile all over again. It's time-consuming and something that you should not [have] to worry about ... ."

The inability to delete a joint account and its content. It was a challenge to be unable to control what happened to the shared account and its content when sharing ended. It was especially hard to control the previously shared content in NDS accounts. For instance, P22-J and her boyfriend at the time created a Gmail account using the combination of both their names as the email ID. They created the account so they could upload their shared pictures on Google drive. Both, therefore, had joint ownership of the account. However, her ex-boyfriend used his email account as a recovery email address, so the account designated him as the account owner. The end of their relationship also coincided with the end of sharing this account. P22-J, who stopped logging into the account after the breakup, remarked: *"... It would be nice if he didn't have [the] pictures [on the shared Google drive anymore] because we're done."* Explaining her current difficulty, she stated: *"... I want to actually get rid of the account, but I can't because it's sort of his account [and] Google doesn't know that it's two people using it. So ... I can't delete [the account]."* Here, while P22-J wanted to stop sharing the account (and to delete its content) altogether, she had no means of achieving this.

The frustration of losing personal content. Some participants reported losing their personal content. P11-P shared her gaming account with her online friends so they could help her play the game. One of the secondary users, however, traded her game characters without her permission. After ending the sharing by changing the account password, she contacted the game administrators to help her reacquire her traded content: *"[The game administrators asked] ... if someone hack[ed] into the account. I said, no, [my game characters were traded away by my friend] because I gave my friend the account [login details]. [The game administrators] said [that there was] nothing [they] could do because [I] voluntarily trade[ed] [my game characters and I] cannot prove that [someone else traded them] without my permission."* For P11-P, there was no means to prove that, while she granted permission to her friends to play the game, P11-P gave no permission to trade her game characters.

Personal content can be also lost when the end of a personal relationship triggered the end of account sharing. For example, P2-P stopped sharing his Netflix account with his ex-girlfriend without notifying her, as he did not feel comfortable bringing this up with her. As a result, his ex lost all of her personalized content (such as her profile) on the Netflix account without notice.

The risk of an account being hijacked by a secondary user. Account hijacking by the ex-partner is a possible risk when a romantic relationship ends. P8-P shared login details for her online dating account (on OkCupid [2]) with her then boyfriend. After they broke up and before she changed her password, her ex hijacked the account and impersonated her: *"[My ex] ended up impersonating me online ... He took control of my account, and he changed the password [and was asking people on my account] to meet up [while pretending to be me] ... I wasn't able to log in [to my OkCupid account], but based on the messages I was getting in my emails, I was able to piece together what was happening."* Issues like hijacking, impersonation, and abuse are covered more extensively in abuse-focused literature [109, 202].

The burden of avoiding awkward conversations. Avoiding awkward conversations was a major reason why participants' attempts at ending account sharing failed. This is because participants were trying to avoid situations where the end of account sharing would signal the end of their relationship. For example, P11-P had an NDS online shopping account with French multinational chain of personal care and beauty stores (Sephora [3]). As a top-level customer, P11-P received more shopping privileges than regular customers, such as free delivery and store promotions. P11-P was sharing this account with her friend. One reason P11-P wanted to stop sharing the account was that her friend occasionally used up P11-P's store points. P11-P explained why she ended up continuing to share the account: *"... if I change the password, she'll know I don't want to share [the account] with her. But I don't know how to tell her! ... She's my friend; I [can't] tell her, 'Stop using [the account], because you annoy me.' It's not a polite thing to do."* P11-P also shared her Apple ID account on her family's shared iPad Mini. When the device was first set up, P11-P found it easier to just use her existing personal Apple ID account

[2] https://www.okcupid.com

[3] https://www.sephora.com/beauty/about-us

than to create a family account. However, she realized later that she had lost part of her privacy, because she was using the same Apple ID on her personal phone, and the users of iPad Mini could see her browsing and search history. Although P11-P wanted to stop sharing the account and regain her privacy, she felt uncomfortable explaining to her family why she wanted to change the account on the device, so she kept using the device as is.

Participants sometimes preferred to stop using an account, rather than having awkward conversations with the secondary users. P23-P, for example, shared her Facebook login details with her friend, but she wanted to stop sharing the account to regain her privacy. However, P23-P felt that deleting the account was a safer option: *"Imagine you were my best friend and then I told you, 'Hey, I want to change the password [because I no longer want to share the account with you], but I don't want to let you know.' I think that's a bit of an awkward situation and [I] don't want to go through that, [so] I asked Facebook to delete my account ... [my friend and I are] still best friends till today."* If P23-P had changed her Facebook password, she would have to explain to her friend the reason behind the password change. P23-P told her friend she deleted her Facebook account because she no longer wanted to continue using Facebook at the time. For P23-P, this was an easier option than to explain that she wanted to stop sharing the account. P2-P did not want to have an awkward conversation with his ex-girlfriend about the Netflix account that he shared with her: *"You know what? I was a coward. I didn't even tell her [I was going to stop sharing the account]. I just went and changed the account plan, and she probably figured out what was happening ... ."*

The stress of ending the sharing of utility accounts when the primary user moves out. Ending the sharing of a utility account was difficult. P6-P, for example, moved out of a household but he was having challenges with ending account sharing, as the Bell internet account "recognized" him as the sole user: *"[My former housemates and I] wanted to transfer the [Bell] account to [one of] my roommate's name [but] we had a lot of trouble [doing that]. It was ridiculous."* Explaining the process, P6-P remarked: *"[To stop sharing the account, my roommate, and I] had to both be on the phone line at the same time ... or we had to go into [Bell] store at the same time, and it's hard because people's schedules are so different. I ended up closing the account, which is more trouble because now we have to mail back*

the modem to Bell, and [my former roommate] has to open up her own account [for the household]." In this situation, the utility company treated the account as a single-user account and hence required a new account to be set up for another household member. Similarly to Moncur et al. [218] we report the difficulty of transferring utility accounts at the end of relationships. The novelty of our work is in exploring these challenges beyond romantic partnerships.

2.4 Discussion

2.4.1 Limitations

Our sample could have been more balanced and diverse. It had more women (64%) participants. We were also unable to get data from older population groups, though we did collect data from multiple age groups. In addition, although we investigated various types of personal relationships, among romantic relationships, we only investigated monogamous relationships.

While all participants stopped sharing at least one online account in the 12 months preceding the study, some of the experiences that participants reported occurred more than a year before the interviews. This may have affected how well participants recalled their experience. Also, only two participants were attempting to end sharing when the interviews were conducted. In addition, as with any interviews, the data were self-reported and may have been affected by a number of systematic biases such as halo effect, social desirability, and acquiescence response bias [79].

Nonetheless, we believe that the results from our study can serve as a basis for further research and technology development in supporting the life cycle of account sharing.

2.4.2 General discussion

The key contribution of this paper is the discovery and categorization of negative impacts of ending the sharing of DS and NDS accounts on users. This contribution may inform the design and evaluation of technology support for various ending scenarios. The prevalence of ending account sharing is yet to be investigated. Most

recent estimates, however, suggest that sharing of online accounts in the US alone is widespread: 22% of Spotify users, 45% of Netflix users, and 64% of HBO NOW users share their passwords [21]. Based on research, most of this sharing eventually ends. For instance, people break up in a romantic relationship or move out of a household. We extend previous studies done on shared online accounts [166, 201, 244], and we contribute to the research on the management of digital possessions after a romantic breakup [155, 218]. While previous research mainly investigates why and how people share accounts [201, 244], we explore challenges involved in ending sharing for both single and multi-user accounts.

Below we highlight two overarching themes synthesized from our results, which characterize user challenges in account sharing and ending.

Access to a shared account could lead to accessing non-shared accounts. In our study, we asked participants about their behaviors regarding their password usage. We do not report all our findings on password behaviors, as they are similar to the previous findings [154, 168, 171, 345]. Our results suggest that people reuse passwords (or use similar passwords) across shared and non-shared accounts. Sometimes, participants seem to forget that their shared accounts have the same or similar passwords with other accounts, as it was with P13-P, who realized that the password for her online bank account was the same as the one for a game account shared with her boyfriend. Besides, some participants reported changing their passwords only when requested by the system, or, occasionally, when they ended account sharing. Access to a shared account, therefore, could facilitate unauthorized access to other accounts. Also, with infrequent password changes, unauthorized users can have access to certain accounts for long periods, which is a security and privacy concern. These concerns emphasize the need for better support of secure account sharing (without sharing passwords) and its ending.

Our results show that the end of account sharing does not always coincide with the end of the relationship. This is in contrast to previous work, which suggests that the end of a relationship implies the end of sharing and vice versa [124, 244, 304]. While we saw this link in those cases when sharing ended because of the end of dependence or loss of trust (also see Marques et al. [198] on trust and sharing), this link did not always exist in our data. In fact, one challenge that primary users faced was finding ways of ending account sharing while still

maintaining their relationship with the secondary user(s). One particular burden was having or avoiding awkward conversations about ending access to the account.

2.4.3 Implications for design

In the next two subsections, we suggest how system design can address some of the challenges in ending account sharing. We acknowledge that there may be non-technical means, e.g., helping people to develop ethical and moral values, or to improve their communication skills. At the same time, technology researchers and developers can explore options for improving support for reasonable use cases and help users avoid unreasonable sharing, while following the path of least resistance.

We believe (but did not verify) that implementing our suggestions may benefit some users and service providers. All the design suggestions could result in improved protection of accounts' privacy and security, as well as better customer satisfaction. Most of these design improvements could lead to a greater sense of control among some primary users, and, as a result, reduce some users' anxiety about their accounts.

Service providers may also benefit, directly and indirectly, from addressing the identified challenges. We expect that improved user experience could result in improved customer satisfaction and fewer customers switching to competing services [283, 313, 329]. More generally, the lower the cognitive and psychosocial cost of securely using an account is, the more compliance budget [18] is left for users to comply with other requirements and rules of the service provider. In addition, service providers might see reduced customer support costs, as the proposed measures may improve account security and reduce abuse and conflict among account sharing users. It should be noted that a thorough analysis of the usability, deployability, and effectiveness of these design suggestions is a subject for future research. Further, we did not consider all user contexts, including abuse contexts, and need further evaluation to determine if and how the design suggestions presented here might work for users coping with abuse or other circumstances not explored in this study.

Designing for ending DS account sharing

Support transfer of user profiles from an existing to a new account. This would reduce the effort needed to transfer profiles and recommendations to new accounts when sharing ends. For instance, when a secondary user of a Netflix-like service is ending account sharing and wants to create their own account with the same provider, the provider could offer the option of transferring the profile to the new account. The transfer can be done by "linking" the old profile to the new account or by exporting the profile data to the user, who can import it into the new account later. This would help users keep their personal preferences, history, movie lists, etc. This is related to the suggestion by Park et al. [244] for romantic relationship maintenance. We go further by offering a more concrete design recommendation. We also note that such support may not only benefit relationship maintenance but could also aid the ending of account sharing. Such a feature could reduce the burden of "branching off" a shared account, which might increase the likelihood a user would continue with the same service provider, rather than switching to a competitor.

Help primary users to remember which accounts they share and with whom, and help them to end sharing if needed. Service providers could support users in these tasks by displaying all the devices that have accessed the account recently or since the last password change, and allowing the user to end account access for some devices. The account could also be designed to allow the primary user to label devices, so that the user can easily identify the devices accessing the account. This design could benefit both the user and the provider by improving the transparency of the access to the account, which might increase the likelihood of the user detecting an account compromise early. In turn, early detection of account compromise might reduce, or even eliminate, the cost of investigation by the provider's technical staff. Some account providers (such as Microsoft, Google, Facebook, and more) already offer some of the features listed, but not all providers do and we note that they would be helpful in many account ending situations.

Allow users to label devices as primary or secondary. This design might grant additional privileges to users when they access the account from a primary device. For example, to help primary users to be aware of which devices are cur-

rently logged into their accounts, the system might also occasionally prompt users (when logged in from a primary device) to log secondary devices out. This account design may benefit users like P20-P, whose boyfriend at the time used her login credentials to log in to the Tumblr app on his phone, but she was not sure whether he could still access her account after the breakup. This design may save primary users from the anxiety of being unsure about access to the account by secondary users. Also, the design may help some users to have a sense of control over which secondary users and secondary devices are logged in to their account.

Allow users to limit the duration of a sign in. Users could also be allowed to set a duration for how long they want to remain logged in. If users do not select this option, then they are automatically logged out of that device after a set time. While a "Keep me logged in" option is available on some accounts, we suggest that developers make it available on all online accounts with the option to specify how long the user remains logged in. For instance, P22-S had been sharing a Netflix account for about 18 months, without the knowledge of the primary user. With this option, P22-S would have been logged out of the account after the set time has expired, protecting the privacy of the primary user.

Ensure that the primary user always stays in control of the account. Sometimes the primary users face a "racing problem" when ending password-based sharing. When account sharing ends, whoever resets the account password first wins the race by taking control of the account (e.g., the ex-boyfriend of P8-P hijacked her dating site account by resetting its password first). This racing problem is also seen in accounts of some banks. For example, to open a joint account at TD Canada Trust, both co-owners need to be present, but either co-owner can close the account (and appropriate the account funds) [15]. We suggest that service providers could make sure that the primary user keeps control of the account independently of the actions by the secondary user(s).

Provide an option of equal account sharing. Our results and studies by others [166] suggest that romantic couples create cloud storage and email accounts that they intend to share equally and use them for digital assets and communications specific to that relationship. The technology could consider providing an option of "equal" sharing, in which a single primary user cannot just "walk away" with the account. This design reassures users that they will not lose the control of

shared digital content when account sharing ends.

Designing for ending NDS account sharing

There are cases of reasonable and unreasonable sharing of NDS accounts. Although NDS accounts are not designed to be shared, participants still shared some of these accounts because they needed to carry out essential tasks that they could only accomplish through account sharing. Since such sharing of NDS accounts does not reduce the revenue of the service providers, we classify it as *reasonable*. More precisely, we define as *reasonable* such cases of sharing NDS accounts that (1) violate the accounts' Terms of Service (ToS) but (2) do not reduce the revenue of the service provider (see Table 2.2). We believe that it would be beneficial (for both the users and the service providers) if it were easier for users to do reasonable sharing of these accounts. We discuss later in this subsection how support for reasonable sharing of NDS accounts and its ending can be improved. We also define *unreasonable* sharing of NDS accounts if it (1) violates ToS and, compared to the case when each user has their own account with the provider, (2) reduces its revenue, e.g., multiple users sharing a single-user Netflix account. This dichotomy of sharing cases is used solely for the purpose of guiding the reader through the discussion of our recommendations, and with the understanding that service providers have many factors to consider when deciding whether and how to support sharing, and our investigation does not explore them all.

	ToS Violated	**Revenue Reduced**
Sharing of DS	No	Not applicable
Reasonable Sharing of NDS	Yes	No
Unreasonable Sharing of NDS	Yes	Yes

Table 2.2: The differences between reasonable and unreasonable cases of account sharing. "ToS" is terms of service.

We suggest that service providers reduce sharing in unreasonable instances by making sure that the path of least resistance [354] for using their products is via non-shared accounts. This suggestion may be difficult to implement, as people circumvent the current barriers put in place to make sharing under unreasonable instances hard. For example, some participants reported sharing Spotify's single-

user account. They used Spotify offline, in airplane mode, when they wanted to listen to songs. This trick prevented Spotify servers from detecting and logging out such concurrent listeners. Participants did so to avoid paying the subscription fee for separate accounts. Apart from lost revenue [63] for the service provider, users' privacy and security are more at risk when NDS accounts are shared. Exploring design trade-offs for reducing unreasonable sharing of NDS accounts appears to be an intriguing open research problem.

Supporting reasonable sharing of NDS accounts.

Some NDS accounts could support safer and easier sharing. As we report in Cognitive burden subsection of Results, P2-P shared his LinkedIn account with his friends and freelancers because he needed help in improving his profile. The availability of many online services that assist users in creating and updating their LinkedIn profiles [175, 196, 262] suggests that many people have similar needs [272]. The participant had to change and remember his new LinkedIn password each time the profile edit was completed and sharing ended. Frequent password changes increase users' cognitive load and nudge them into the unsafe behavior of sharing their passwords with others. It also likely uses up their security compliance budget [18], which can lead to choosing easy-to-guess passwords or even reusing passwords across their accounts (as our participants reported). Findings from our and other studies [198, 201] suggest that users share their social media accounts for convenience and to signal trust (see Results section and Table 2.1). For example, a friend of P18-S shared his Facebook and Instagram accounts because he wanted P18-S to check his social media messages, to help him keep in touch with his contacts during exams and other hectic periods of his life. In this scenario, it was convenient for the user to share his account, but doing so by sharing his password was unnecessary.

Support password-less sharing of account personal content. Rather than pushing users toward violating terms of use (which make users to agree to "(1) try to choose a strong and secure password; (2) keep your password secure and confidential" [188]), LinkedIn, Facebook, and similar services could create easier means for users to provide others with access to (parts of) their profile/content without

sharing the passwords for their individual accounts. For instance, LinkedIn could design users' personal accounts to have sharing functionality, similar to Google Docs, Overleaf [4], or Facebook Business Pages [5]. Users would be able to share their personal content (in this case users' social networking profile or personal posts and direct messages) by granting others edit or review rights. Since our and others' findings [99] indicate that passwords are commonly reused across online accounts, eliminating cases where users have to share their passwords may benefit both users and service providers by improving security of the accounts.

Support granting of fine-grained permissions to other users. We recommend that users be able to give fine-grained permissions rather than an all-or-nothing access to their personal content. Social networking sites could design personal accounts to enable users to give other users the right to view and/or modify certain parts of their personal content. This could include being able to view messages, reply to messages, and make posts on the shared accounts. To end the sharing of the accounts, the primary user would remove the permissions of the secondary user(s) in the account settings.

These designs may be beneficial to both users and service providers. This is because for some users, the cost of changing passwords is higher than the cost of giving secondary users the right to edit a profile. With such designs in place, users would not even have to share their passwords to begin with. Therefore, ending account sharing could be simplified without primary users changing their passwords for the shared account or remembering to avoid using passwords similar to the ones on their other accounts. This design could also reduce users' cognitive load (and indirectly the use of their compliance budget) due to remembering new passwords. The feasibility of this suggestion has been demonstrated by Twitter, which has recently enabled multiple users to share a personal account without sharing its password [325]. Further, shared passwords give full access to the user's account, which violates the principle of least privilege [295]. This design may also benefit the company by reducing customer support costs arising from secondary users hijacking accounts.

Design household utility accounts with multiple users in mind. There are

[4] www.overleaf.com/about

[5] www.facebook.com/business/pages

many challenges involved in using a single utility account. There is an entanglement of service accounts (i.e., accounts used for providing services) and user accounts that hold billing transaction history, preferences, and information specific to the user. This entanglement needs to be removed to support the ending of sharing utility accounts. We suggest that each household could have a set utility account, e.g., "Apt 131 Electricity," and the system would be designed to support Relationship-Based Access Control (RelBAC) [16]. For example, when people move into apartment 131, their individual accounts are added to the "Apt 131 Electricity" utility account, and at least one person is designated as a primary user. With RelBAC, the primary user can assign other users to specific roles. To end sharing when a user moves out of the apartment, a primary user would remove that user from the shared account. Such a design would benefit users by making it easier to transfer the responsibilities for the account. Also, apart from reducing the support cost for the company, the cost of closing one shared account and opening another one may be less for both users and the utility providers. There may also be higher customer satisfaction.

Support household accounts on shared devices. We suggest encouraging users to set up multi-user "household" accounts on shared devices, rather than sharing single-user accounts, by explicitly designing support for such accounts. For example, while Apple provides a "Family Sharing" capability to support the sharing of purchased content across individual accounts [8], it requires each device still to be activated with one individual's Apple ID. As our data suggests, privacy issues arise when single-user accounts are used on the devices shared in households, and, with time, the psychosocial burden of ending the sharing of such accounts only increases. Device manufacturers and service providers could consider making household accounts first-class citizens. One option could be to include a step during the device setup process to indicate whether the device is designated to be shared. If so, then the device could be specifically configured for sharing, so that each user would use their own account/profile on the device. A benefit for the users could be the protection of their privacy and security, which is particularly important given the potential threat from social insiders [197, 198]. Even though service providers may prefer that each user possess their own device, our and others' findings suggest that sharing of devices is common [201]. The potential improvement

in user experience and reduction of psychosocial burden could benefit users and, indirectly, the service providers.

2.5 Conclusion

We report various security and privacy challenges involved in the ending of account sharing in personal relationships. Our findings suggest the need for developers to consider the various challenges and the different contexts when designing online shared accounts.

Chapter 3

Security and Privacy Challenges of Mass Telecommuting

This chapter reports the security and privacy challenges and threats that people experience while working from home. Our research aims to provide insight into the security and privacy concerns associated with telecommuting to help employees safely work from home while protecting organizations' confidential information. Our research question (RQ 2) is: what are employees' security and privacy challenges, threats, and perceived risks when working from home? We conducted semi-structured interviews with 24 participants working from home in the three weeks preceding the study. We asked questions related to participants' challenges with telecommuting. Our results suggest participants experienced challenges, threats, and potential risks broadly associated with the technological and human dimensions. We also discovered two threat models: one in which the employer's asset is at stake and the other in which the employee's privacy is compromised. We believe these insights can lead to better support for employees and possibly reduce cyber-attacks associated with telecommuting during the COVID-19 pandemic and beyond.

Key contributions of this chapter are:

- We performed the first qualitative study on employee security and privacy concerns when telecommuting. We identified the perceived risks associated

with these concerns. We grouped our findings into four categories technological, human, organizational, and environmental dimensions. In addition, we grouped our findings into the identified security and privacy risks and showed the threat models that emerged from our results.

- Second, we discovered concerns that need to be addressed to protect employee privacy while telecommuting. For instance, it is difficult for employees to draw the line between their privacy and getting work done-which in turns maintains their professional relationship. On the one hand, employees want to maintain their privacy. On the other hand, employers expect employees to conduct their regular work activities at home, including employees giving clients their personal phone numbers and risking being scammed. Participants also had a constant fear that clients could locate their home or that they could suffer from a break-in. Therefore, there is a needed form of discourse around how employees and organizations can protect their privacy and security while telecommuting.

3.1 Definition of Terms

For the sake of clarity, we define some terms. Challenges and threats are often used interchangeably; however, they do not necessarily mean the same thing. In this paper, we define a threat as "an event or condition that has the potential for causing asset loss and the undesirable consequences or impact from such loss" [284]. A challenge is a circumstance that could lead to a threat. And an outcome of a threat is "an expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result" [301]. These outcomes could be loss of organizational data confidentiality, integrity, availability, or personal privacy loss. We define confidentiality as "the property of non-public information remaining accessible only to authorized parties" [331]. Privacy "more narrowly involves *personally sensitive* information, protecting it, and controlling how it is shared. ... What information should be private is often a personal choice, depending on what an individual desires to selectively release." Integrity is defined as "the property of data, software or hardware remaining unaltered, except by authorized parties" [331].

3.2 Related Work

Telecommuting and telework are similar but different. Whaley [343] defines telecommuting as "using information and communications technologies (ICTs) to bring work to the worker, rather than require them to go to the work." In telecommuting, the employee does not commute to get to work. Examples of telecommuting could be working in the home office or working out of the office in the home environment, for example, the guest house. On the other hand, telework refers to work that is done somewhere that is a distance from one's office. Examples of teleworking could be working at another branch of an office or working at a telework center with other colleagues. While some types of telework are telecommuting, not all types of telecommuting are telework [282, 343].

Many previous papers focused on teleworking benefits and aimed to understand problems that stop its widespread adoption by organizations. For instance, Pyöriä [265] conducted a literature review on the advantages of distributed work, which the author refers to as telework. Similarly, Kintner [174] conducted surveys with 1,002 respondents to determine how receptive businesses were to telework and identified ways to encourage managers to telework. The respondents were workers in various organizations who were not teleworkers. The author identified issues that prevented telework adoption, such as inadequate security for protecting transmitted information while teleworking, the high cost of buying the needed equipment, and the lack of staff available to aid telework transition, among others. Our study builds on previous research and conducts qualitative research with telecommuters. We chose to interview telecommuters to understand their security and privacy challenges and threats when working from home.

Some papers explored the reasons behind the low adoption of telework before the pandemic. One of the reasons for low adoption was poor data security. Clear and Dickson [62] for instance, studied whether telework adoption was influenced more by levels of worker autonomy, employment flexibility, and management attitudes than technology provision. The authors conducted 303 surveys and 58 interviews with representatives of small and medium enterprises (SMEs). In discussing their results, the authors remarked that data security is "a major disadvantage to the adoption of telework." However, the authors did not explain why this was the case.

Spinellis et al. [309] also hypothesized that SMEs lacked the potential to have good technical expertise to maintain an adequate security level in teleworking. The work of Pyöriä [264] is closest to ours. This author conducted a survey and interviews with employees to understand the low adoption of telework even in big organizations. The participants, however, were not teleworkers. The authors categorized their findings into those relating to the individual, the organization, and the community. They described the pros and cons of telework at each level. The findings relating to the organization level are closest to our findings. The author found that some of the drawbacks of teleworking include the problem of employers seeking new means to surveil and control employees, poor data security, and disruption of privacy in employees' homes. Our work differs from Pyöriä's [264] in two major ways. First, we interview employees who are currently telecommuting. Our focus on telecommuting employees helped us to understand the specific challenges these people are facing. Further, building on Pyöriä's study, we focus on telecommuters' security and privacy concerns and find more challenges and threats. Because of the potential for a number of telecommuters to continue for the long term, our research becomes even more critical.

Several papers focus on the security and privacy challenges of telecommuting. However, these papers are not based on empirical data but on hypothetical situations. For instance, one of the earliest papers on telecommuting was written by Sturgeon [312]. The author used a hypothetical case study to highlight vulnerabilities. The author predicted threats and risks to organizations' confidential data when telecommuting using the Simplified Threat and Risk Assessment Process [312]. A more recent paper by Okereafor and Manny [234] provides an overview of security issues that are related to telecommuting and videoconferencing apps. The authors predicted issues related to workers' geographic location such as workers' telecommuting in locations with poor Wi-Fi networks and workers being distracted while working from home, which could lead to dangerous errors. The authors also highlighted other general issues such as telecommuting devices using a lot of bandwidth and reduction in employees' productivity while working from home.

Our paper is the first to provide a qualitative study on telecommuters to understand their security and privacy challenges, threats, and perceived outcomes of threats. We chose to conduct a qualitative study to understand *why* people face

some of the predicted challenges and *how* they experience them. Qualitative studies help answer "why" questions and provide an in-depth understanding of what is being studied [270]. We believe that a more in-depth analysis of these concerns will help researchers better understand the challenges and start a discourse on ways of addressing them.

3.3 Methods

3.3.1 Participant Recruitment

We recruited participants by advertising on Facebook, LinkedIn, and Kijiji using the platforms' paid advertisement functionalities. Potential participants filled out an eligibility survey. To be eligible to take part in the study, participants had to be 19 years or older. Participants had to have worked full-time physically in an office space in the year preceding the study. Participants had to have been working with computers for at least three days a week, so that we could explore current challenges they might be facing with the technology. Further, participants had to have been working remotely full-time in the last three weeks preceding the study. The latter inclusion criteria was to ensure that participants would remember recent experiences with working from home.

3.3.2 Participants' Demographics

ID	Age	Gender	Educational level	Place of work	Position at work	Number of employees	Location
P1	24	W	Bachelor's	University	Digital communications specialist	-	Montreal, Quebec
P2	32	W	Master's	Library	Manager of marketing and communications	-	Montreal, Quebec
P3	31	W	Master's	University	Research assistant	14	Kitchener, Ontario
P4	36	W	Master's	Community organization	Occupational therapist	2,000+	Mount Pearl, Newfoundland
P5	49	W	Master's	IT firm	Sales director	10,000+	Caledonia, Ontario
P6	51	M	Bachelor's	Provincial government	Senior staff	-	Halifax, Nova Scotia
P7	47	M	High school	High school	Network engineer	11,000	Mono, Ontario
P8	61	M	Bachelor's	Children's science museum	Accounting supervisor	101	Vancouver, British Columbia
P9	24	W	Bachelor's	Federal tax agency	Call center agent	40,000	Ottawa, Ontario
P10	38	M	Bachelor's	Realtor	Mortgage broker	11,000	Mono, Ontario
P11	52	M	Bachelor's	Community center	Health director	85	Port Hardy, British Columbia
P12	31	M	College	Telecommunications	Account manager	-	-
P13	25	W	Bachelor's	Car sharing service	Business operations manager	22,000	Vancouver, British Columbia
P14	64	M	Bachelor's	Cannabis producer	Call center representative	37,000+	New Maryland Parish, New Brunswick
P15	31	M	Bachelor's	Telecommunications company	Customer service rep	37,000+	New Maryland Parish, New Brunswick
P16	47	M	Master's	Public transport services	Director in the planning department	4,000	Toronto, Ontario
P17	38	W	Master's	Elementary school	Education assistant	-	Dawson Creek, British Columbia
P18	38	M	College	Arts and culture management organization	Executive director	3	Vancouver, British Columbia
P19	43	M	Bachelor's	University	Business support analyst	10,000+	Vancouver, British Columbia
P20	30	M	Bachelor's	College	Assistant registrar systems and reporting	-	-
P21	53	M	Master's	Securities commission	Senior project manager	-	-
P22	48	M	College	Telecommunications provider	Customer service call agent	-	-
P23	59	W	College	High school	School secretary	-	-
P24	24	W	College	High school	School teacher	35	Halifax, Nova Scotia

Table 3.1: Demographics of participants.

3.3.3 Interview Procedure

We proceeded with the interviews after the participants gave informed consent to participate in the study. To avoid priming, we told participants that the aim of the study was to understand their experiences working from home.

We asked participants for demographic information and about their general experiences working from home. Based on these experiences, participants were asked further questions regarding what they enjoyed about working from home and what they would love to change about their experience (if anything). Participants were also asked to list new technologies that they had been using to work from home. We asked further questions about participants' thoughts about using the technologies (see Appendix B.1). Afterward, we compensated the participants. One or two researchers took part in each interview session. All interview sessions were audio recorded.

3.3.4 Data Collection

We piloted our study procedure with two participants. Based on the feedback from the pilot interviews, we improved the clarity of the questions. All other instruments in the main study remained the same as those used in the pilot.

We carried out semi-structured individual interviews with all recruited participants. This allowed them to express their thoughts in their own way and to add information as they saw fit, without the restrictions of structured interviews [65].

All interviews were conducted either via Skype or Zoom, based on participants' choice. We chose to conduct online interviews due to the restrictions placed on in-person meetings resulting from the COVID-19 pandemic. Participants were compensated with CAD $20, sent via e-transfer. Data collection was done from March to September 2020. Our university's Behavioural Research Ethics Board (ID: H20-01219) approved the research before any data collection took place.

3.3.5 Data Analysis

Two researchers transcribed and coded more than 18 hours of recorded interview sessions, each an average of 44 minutes long. Interviews were analyzed using thematic analysis [126], a "set of procedures designed to identify and examine themes

from textual data in a way that is transparent and credible" [125]. We followed the data analysis steps outlined by Guest et al. [125]. Two researchers segmented and coded the transcribed interviews into categories, types, and relationships to develop the codebook. Afterward, three researchers identified the themes that emerged from the data. In addition, four researchers engaged in a code and theme sorting exercise to come to a consensus on the identified themes. We conducted data analysis concurrently with the collection and reached theoretical saturation after 21 interviews, as no new codes emerged from the last three data collection sessions (see saturation graph in Figure 3.1).

3.4 Saturation Graph

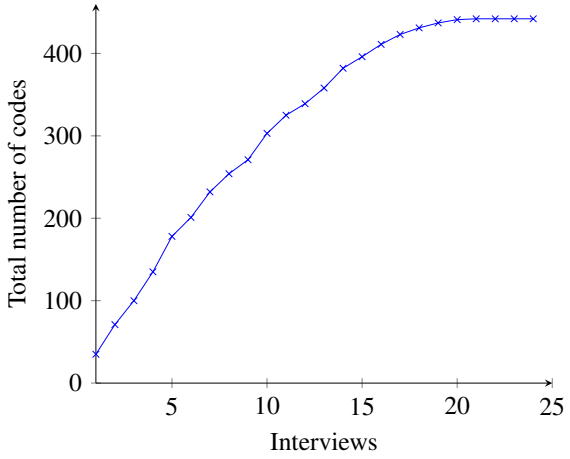

Figure 3.1: Total number of codes after each interview.

3.5 Results

We present our findings in the form of the challenges and perceived threats, which we categorized into technological, human, organizational, and environmental dimensions. We also link them to perceived outcomes of threats.

3.5.1 Participants

We recruited a diverse set of 24 Canadian participants. They were 19 to 64 years old (mean 41 and median 38), with 14 of them identified as men. Table 3.1 shows the demographics of the participants regarding age, gender, educational level, place of work and job, as well as size of the employer and geographic region (when available).

3.5.2 Technological Dimension

Challenges related to technological dimensions are due to the use of technology while telecommuting. These challenges could result in threats to the security and personal privacy.

Sharing work information in unauthorized ways

Some participants used unofficial online communication channels to share work-related information. This action was a security concern as it was unclear whether these unauthorized technological solutions satisfied employers' data security requirements. Since different communication solutions have varying degrees of compliance with organizations' security and privacy requirements, using these solutions could lead to various security and privacy threats for both the organization and its employees. This action could also lead to the outcome of threat of the loss of the data *confidentiality*.

One reason for using unauthorized channels was **low usability of the authorized channels**. For instance, P15 (customer service representative) was supposed to use Bell Total Connect (BETC). However, he found it unusable: *"[To use BETC] you've got to request access, then you download it, and then you've got to have your credentials in place. ... It's a complicated program."* P15 ended up using Facebook and sometimes text messages to communicate work-related information with his boss and colleagues while telecommuting.

Another reason for the use of alternative communication channels was because **most of our participants' colleagues were already using them.** It was therefore easier to reach colleagues there. P14 (call center representative) explained: *"We do have a chat [function] in our [official] program, [but it's] just that everybody's on*

Facebook Messenger. So whether you like Facebook or not, you're kind of forced to use Facebook. And so I [use Facebook since] everybody's there."

Sacrificing personal privacy and security

There were many instances where participants sacrificed their privacy or security to telecommute. We discuss these instances below.

The tension between professionalism and privacy on video calls. Many participants experienced tension and uncertainty around the use of their webcams during work meetings. For the sake of personal privacy, participants wanted to keep their video cameras off during some periods of work calls. However, they were uncertain whether doing so made them appear less professional or serious about their job. For P16 (planning department director), having the webcam on during work meetings was a necessity, although his colleagues did not necessarily agree: *"People should be available on video if they're doing work during the workday. [However,] that [is] a concern for some people. I have a colleague, and today she said, 'I can't show you my video because my hair is in an Afro.' ... Maybe she didn't want people to say something, or to notice, or to make a case out of it."*

P21 (senior project manager) also explained the dilemma: *"I can't force [people to turn their video on]. It's their home, so I can't really force them; I can only insist. I know that some of the managers in our organization make [a] point of telling [employees to] turn [their video] on during the meeting, [because the employees] have to be paying attention."*

Some participants felt that having the video camera on was an invasion of their privacy. Participants feared that people could take screenshots of them without their consent. P18 (executive director), explained this concern: *"I've thought about [people taking screenshots during video meetings], 'cause I know people who have [done that]. I have a call every two weeks, and there's usually about eight or nine of us [on the call], and I know that they're taking screenshots of the video [meeting], but I wish ... a part of me feels like, there should be a notification feature [on the teleconferencing app that shows] if somebody's doing a screenshot [during meetings] or if they save an image. My preference is that people ask if they're going to do a screenshot for whatever reason."* Having webcams on also

virtually invited co-workers into participants' homes, which was seen as a privacy invasion. P5 (sales director) explained: *"[Through video calls,] you're inviting a lot of people into [your] home that [you] wouldn't have otherwise. So you're here [on the video call], your kids are walking by, or other family members or your dog or whatever the case may be, [and] you may not want people to see [all of that]."* P3 (research assistant) further explained: *"[Work video meetings] certainly blur that line between your home life and your workplace. Like right now, you're in my kitchen with me. Normally co-workers wouldn't necessarily be inside the house, which is sort of a weird ... it changes that relationship [with my co-workers]."* Having webcams on during work meetings leads to the loss of employee's *privacy*.

While some of these challenges can be solved using virtual backgrounds [303, 318, 359], participants had issues with the availability and usefulness of virtual backgrounds. First, not all videoconferencing apps fully support virtual backgrounds [209]. Second, not all participants liked the idea of using a virtual background as they found the concept of virtual backgrounds to be too dull or unexciting. Third, virtual backgrounds do not guarantee that people walking by will not pop up on the screen [279].

The design of some tools made it difficult for employees to maintain security while working from home. This challenge sometimes led to the organizational outcome of threat of the loss of the data *confidentiality*. For instance, phones that used the same port for charging and connecting headphones were a challenge in case of long and frequent calls: *"I think the biggest issue [with working from home] for me is [my phone]. If I've got a day that is heavily focused on a lot of client stuff, then I have to continue using my work phone, which can be problematic ever since they've got rid of the bloody plugin that you can put your headphones in and [replaced] it with [one port], because that's [the port] I need to charge my damn phone with. So I have, on occasion, had it plugged in [to charge] and used it without headphones. And technically, depending on the voice tones of the other person [on the other end of the phone], somebody may have [over]heard our conversation."* [P11 (health director)]. This was a security concern because housemates could overhear confidential information (§3.5.3). The participant sacrificed the confidentiality of his work calls to get the job done. In some cases, to use headphones and maintain security, P11 switched from taking calls on his work phone

and used his personal phone instead. However, our results also suggest that using personal phones to manage work conversations could be a security and privacy concern, as we explain below.

Employees share their personal information to aid telecommuting. Some participants shared personal phone numbers or home addresses with colleagues and clients. In some cases they used their personal devices to work from home. These actions sometimes made it difficult for participants to draw the line between their personal and work lives. P8 (accounting supervisor), for instance, could not "move" his work landline home. So he gave the clients his personal phone number. Prior to working from home, P8 never picked up calls from unknown numbers because he was afraid of being scammed. That changed after giving his personal number to work clients: *"[Recently I received a call from an unknown number.] First ... I wasn't going to answer [but] then I [decided to] answer [and] I was really lucky that I took the call because it was [from] the government. And [the government] was just verifying information so that they could pay [my organization] the subsidy. So if I'd refused that call, it would have really slowed down the payment, and then my boss would have been mad at me, because we were rushing around to submit our application. So of course now I'm answering more calls on my [personal phone], and I don't screen it as closely as I [used to do] before. If I'm going to work from home, that's part of working from home. I'm going to pick up the phone for numbers that I don't know."* P8 sacrificed his privacy and precautionary safety measure to continue his regular work activities at home.

When asked if he still had a fear of picking up a call from a scammer, P8 replied: *"I'm afraid if I pick up [a] call from a scammer, that somehow they are going to know that there is a live person at the end of the line and then they're going to get me more scam calls. [But] I'm afraid that if I miss a business call, then I'm going to get criticized by my boss because it affects my work, [and] I [end up not] do[ing] something [at work] fast enough. And the boss will be mad, because I didn't pick up a phone call."*

P23 (school secretary) further remarked: *"I had to use my own personal cell phone to communicate with parents. That part of [telecommuting] was awkward ... because now I find the parents text me or leave me a message to get information. For me [giving out my phone number] does cross the boundary. I always have tried*

to separate as much as I could, my private life from my work life ... it was basically just assumed upon us [by the organization] when [the organization] decided they were going to [send us home to work]. ... I probably could have done [the call blocking code], but I didn't do that. I do believe you get charged for [doing that] so I didn't want to have that fee on top of other fees."

In some cases this challenge included giving coworkers participants' home addresses. P3 further explained: *"So if I asked my coworker to pick something up from my office, then probably he might drop it off at my house. So then he would know where I live. So I feel like it starts to open up some kind of personal privacy [issue]."*

The use of some technological tools in telecommuting made it easy to monitor participants' activities. For example, the User Presence feature [320] in Microsoft Teams makes it easy to determine a user's activities online. Some participants were concerned of their *privacy* being further reduced by this feature, as illustrated by P16: *"I notice that you can tell who is on their computer and who is not, [using Microsoft Teams]. For example, now I can type any name, and I can see [who is online and who is not]. [The] red [button] means that they're on a [Microsoft Teams] call or [in] a meeting; green means that they're on their computer, but not in a meeting. And yellow means that they've walked away from their computer and the little X means the computer's turned off. I find that [that] can be used to monitor whether people are at their desk or not. So, for example, a manager can check whether their employee is yellow, green, or red, and they could be green and surfing the 'net, and they could be yellow and reading a document [on] the computer. ... [Managers] might jump to conclusions [in] thinking that an employee should be either green or red, but not yellow, because yellow means that they're not [at] the computer."*

Unauthorized people controlling participants' computer remotely. The possibility that people's computers could be remotely controlled was a privacy and security challenge for participants. Some jobs require participants to give their employers or customers remote access to their computers. However, in giving employers remote access, participants feared that their employer would be able to access other parts of their computers remotely which could lead to *unauthorized access to data* and loss of *privacy*. When teaching students online, the job of P17

(education assistant) requires her to give her students remote access to her computer so that they can play an educational game: *"When we are sharing the screen with [another] person, we ... give [remote] control to the other person, [and] that was [a] concern because that person can go on your computer and probably check anything on your desktop. [For example, after giving remote control to a student], then that student can control my screen ... or can check anything."*

Reducing security for usability

To make some technological tools usable, security was sometimes sacrificed. We discuss some instances where security and privacy were sacrificed for usability while telecommuting.

Employees bypassed organizations' security measures to make use of technological tools. As a security measure, some work-from-home phones were too locked down, and participants did not find them usable enough. Participants sometimes came up with workaround solutions that were less secure. These workarounds would result in even higher consequence of threat to the *confidentiality* of the organization's data than the task they were trying to accomplish, as illustrated by the story of P6 (senior staff): *"The [work] iPhone that I [use] is so well locked down that I cannot copy and paste from an email into a text message. [If I try to do that, the work iPhone] says 'You cannot paste your organization's data here,' and it's a complete pain because there are times when [I'm] communicating with my boss by text message where she says, 'Can you just send me that phone number?' [or] like an email address or something like that. [I] can just type [the information my boss is asking], but my memory is terrible. I would always copy and paste something rather than [type] it. [It's] a particularly annoying feature and so I found a workaround: If I had something that I needed to text to my boss, I [would] actually send the email from my work email address to my home email address, then use my [personal] iPhone to cut and paste the information into a text and send."*

Reduced security of technology to aid usability. To enable employees to work effectively from home, sometimes IT personnel reduced the security of some organizations' devices. Such compromises could reduce organizational data *confidentiality* and *integrity* and violates organization's security control rules and poli-

cies. P8 narrated a related experience: *"[I] brought [a second] monitor home when I first remote accessed [in to work]. The second monitor did not work, and so I complained to the IT manager, and [the IT manager] said [that] for security purposes the standard remote logging software simply does not allow two monitors. So the IT manager said, '[P8's name], don't tell anybody else this because it's not good control, but I made you a special URL, and now you can access [the work computers remotely with] two monitors.' I'm guessing that by giving me this special URL [designed just] for me, I have more access to the [organization's] information... . So I think it's weaker control over the security of [people's] information.' And [the IT guy] did tell me, 'Don't tell anyone else; I'm just doing this as a favor for you,' because IT [has] to maintain the security of the computer network. And if there was a hack or break-in, [the IT manager] would get blame[d]. So I have not told anyone else, but really I should tell my colleagues because it would speed up their work, [but] I'm afraid I'll lose the special favor with the IT manager if I tell anybody else."*

3.5.3 Environmental Dimension

There were threats specific to the home work environment. They were mostly expressed as fears and concerns. We describe these threats below.

Household members can access the organization's confidential information

There were concerns about others in the household overhearing the organization's confidential information. This was a particular concern for participants with housemates. In some cases, participants shared office space with their housemates. In other instances, the house had thin walls, and the house occupants and guests could overhear conversations held in various locations within the house. Some participants' jobs included handling confidential information; therefore, a security threat was that others could overhear these conversations. This led to the organizational outcome of threat of the loss of data *confidentiality*. For instance, P15, who had three roommates and worked from the dining area of his house, explained: *"If [clients are] giving me [their] credit card information, and I'm reading [the credit card details] back to [them, I would be] around people [in the house while reading*

the details]. Frankly, I don't think I'll be able to avoid [my roommates' overhearing] until I go back to the office. ... Right now, if somebody comes into the kitchen [to] make food, I could be on a call, [and] that makes things a little awkward at times."

Participants feared that their customers and colleagues could overhear private conversations from participants' homes. They were concerned with the loss of their and other housemates' *privacy*. P9 (call center agent), explained this concern: *"We have very thin walls in my house, and my room is right beside the bathroom. And a lot of times when my parents are calling [for] my brothers' [attention], I can hear [my parents] through the wall. Sometimes I have text[ed] my brothers [saying], 'Hey, can you please keep it down? I'm on the phone with a taxpayer. And they may be able to hear you through my headset.' [At] home you can almost hear everything that goes on."*

There was also the possibility of unauthorized people viewing employer's confidential data. For instance, P11, who worked from his dining room, explained: *"[I] had multiple eye surgeries last year, so I don't really see out of this [eye]. So I have a big screen in our dining room, which is completely open to our kitchen. And then [on] another side, it's kind of an open concept: living room, dining room, [and] kitchen. If anybody was coming in and walking around, they could have seen documents that I was working on the large screen, because it blows it up quite large, so it's quite legible to anybody that wanted to read it."* This is a security threat, as P11 sometimes works on clients' confidential information.

Employee's location could be traced

Some participants feared that some of the work calls made from home could be traced back to their location. This would result in the loss of their *privacy*. To illustrate, P9 works with the government and sometimes takes phone calls from angry citizens. While telecommuting, P9 uses her work mobile phone to make and receive calls from clients at home. P9 remarked: *"Sometimes, I wonder if [clients] are able to trace my phone calls. I know they're not [able to] because my [work] phone number doesn't pinpoint the exact location I am in. I work with [people's social insurance/security] numbers [and] addresses [on my system, and]*

a lot of the times when I get calls, some of them I realized have been close to my neighborhood. There was one call I received that was actually two streets down from where I was staying. And I [thought], '[What] if this person knew where I was located?' Sometimes I wonder, 'Oh, man, like if they knew where I was located, would they come to my house and ask me to do stuff?" While this threat may be improbable, this fear made the participant anxious about handling work phone calls from home.

People might break into employee's house

There was a fear that someone could break into participants' houses to steal the company's equipment. This was a security concern and a constant fear for few participants who took home expensive work devices to aid telecommuting. If realized, this consequence of threat could result in the violation of participants' *privacy* and safety, loss of system *availability*, as well as data *confidentiality* and *integrity*, and, in extreme cases, the loss of *life*. For instance, P11 explained: *"My only other massive fear is, what if I had a break-in and somebody stole my [work] laptop? I mean, I have great confidence that that wouldn't happen, but it absolutely has been a fear. I think that's probably [the] only sort of ... situation that genuinely creates the occasional bit of anxiety for me ... 'Jesus, how do I know I am [secure]?' [Someone breaking in] seems like one of those improbable situations, but not impossible. So, even saying it out loud makes me nervous that somehow I am creating that reality now, because we certainly have people [in my neighborhood] with addictions who sooner or later need to feed their addictions and need to get money and sometimes get desperate."*

3.5.4 Human Dimension

These are challenges that were specific to individuals and their varying capabilities or limitations. We explain these challenges below.

Challenges with using the technology

Some participants were not tech-savvy, which made it harder for them to switch to full-time telecommuting. P7 (network engineer), for instance, remarked: *"The*

human aspect of security is always the biggest problem. [The IT personnel] are not there to monitor what everyone does at home on their computers all the time. Users don't know how to properly explain what their [technological] issue is; they use end-user terminology instead of technical terminology. So trying to translate the communication with the users was the biggest challenge. [When users had a technical issue,] trying to get them to explain to us what the problem [was challenging]."

Lack of technical knowledge could lead to dangerous errors. This outcome of threat was particularly a concern when there was a disconnect between the participants' knowledge and what the organization expected them to do. For instance, some participants could fail to install security-critical software updates on their work systems while telecommuting, due to the lack of the technical capacity to do so. This challenge could lead to the loss of *integrity* and *confidentiality* of the organizational data, should employees' computers become targets of cyber-attacks.

The lack of technological competence was also reflected in poor understanding of security. For example, when discussing virtual private networks (VPNs), P1 (digital communications specialist) remarked: *"VPN, is ... something that secures your laptop. I just know [VPN] makes everything safe. You can't get hacked. You can't [have] none of that [hacking]. Everything's secured."* In this particular case, P1 assumed that once she connected to her employer's network using a VPN, everything on her laptop was secure.

The challenge of distinguishing real organizational emails from phishing ones

Participants had difficulty distinguishing between real organizational emails and phishing ones. Sometimes, employees had been so much sensitized about phishing emails that they would classify real organizational emails as phishing. P7 shared an illustrative story: *"[Prior to working from home, my organization had [a] service that would do hands-on training [and send] out test fake emails to [employees]. If anyone clicked on [one of these fake emails], they'd get a warning, that [said], 'By the way, this is not real; this is a phishing email.' Now, [while employees have been working from home], we were sending out updates regarding viruses and anti-viruses and then people were reporting [them] as [phishing emails], not realizing*

it was a legitimate board email. [People have become] too paranoid."

It was hard for some participants to recognize legitimate work-from-home precautions and apply them as needed. Some of these precautions are required to protect the confidentiality and integrity of work data. Therefore, similar to the challenges of using technology (§3.5.4), this challenge could lead to the loss of *confidentiality* and *integrity* of organizational data.

3.5.5 Organizational Dimension

The major challenge was that organizations sometimes provided few or no guidelines on how to telecommute. We define telecommuting guidelines as a set of instructions for employees about what to take home from work, how to set up their home office, and how to ensure the security and privacy of work-related information. We discuss this challenge below and explain how it led to other security and privacy issues for participants.

Many participants received little or no guidance on telecommuting. P15, for instance, was handling financial information while working from home. However, it was unclear to him how he would do that safely. When asked about guidelines regarding working from home, he explained: *"We barely get told anything [regarding telecommuting]. ... There hasn't been any communication with regard to how to handle confidential conversations over the phone. We just use our discretion [in handling financial] matters [over the phone].*

Telecommuting violates the organizations' work policies. For some organizations, working from home violates the organization's policies, and therefore, there are no guidelines for employees. When P11 was asked about the work-from-home guidelines instituted by his organization, he remarked: *"There were no guidelines [for telecommuting;] in fact, ... [working from home] is breaking [the] guidelines. ... We had just recently completed a very thick policy manual about data protection, information, privacy, [and] security ... that indicated [that] you don't take anything [from] work [to] home. All work will be done from the office. So in fact, having to respond to the pandemic created a conflict with recent policies around the security of information."* As such, people in some organizations had no guidelines on how to work from home.

Participants, therefore, came up with their own norms of working from home. They used their own understanding and interpretation of security and privacy best practices. For instance, when asked about her work-from-home practices, P3 explained: *"[Be]cause I'm working on my personal computer, [I'm] not saving anything on my actual computer a whole lot. ... I save everything on my [USB] stick. It's not too hard [to remember to save files on my USB stick] because I just leave the stick plugged into my computer ... so it's right there."* P3 further explained that she secured her laptop by using a password, though her USB stick was not encrypted or password protected. Since P3's USB stick was always plugged into the computer, the information saved on the USB stick was only as secure as the information saved on her personal computer or even less. The concern is that attackers (who could be household members) need a password to access the files saved on P3's laptop, but attackers can easily access the USB stick files. This challenge could lead to the organizational outcome of threat of the loss of data *confidentiality* if attackers had access to the USB stick.

3.6 Discussion

3.6.1 Limitations

Our sample could have been more balanced and diverse. It had more male (56%) participants, though statistics show that more men are employed than women [239]. The average and median age were 41 and 38, respectively. We could have recruited more older participants. However, the oldest participant was 64, and statistics show that on average the age of retirement is 62 [44, 298]. Furthermore, as with most qualitative research, the data were self-reported and may have been affected by several systematic biases such as social desirability, halo effect, and acquiescence response bias [79]. Nonetheless, we believe that our study results can serve as a background for further research and discourse on how to improve the security and privacy of telecommuters.

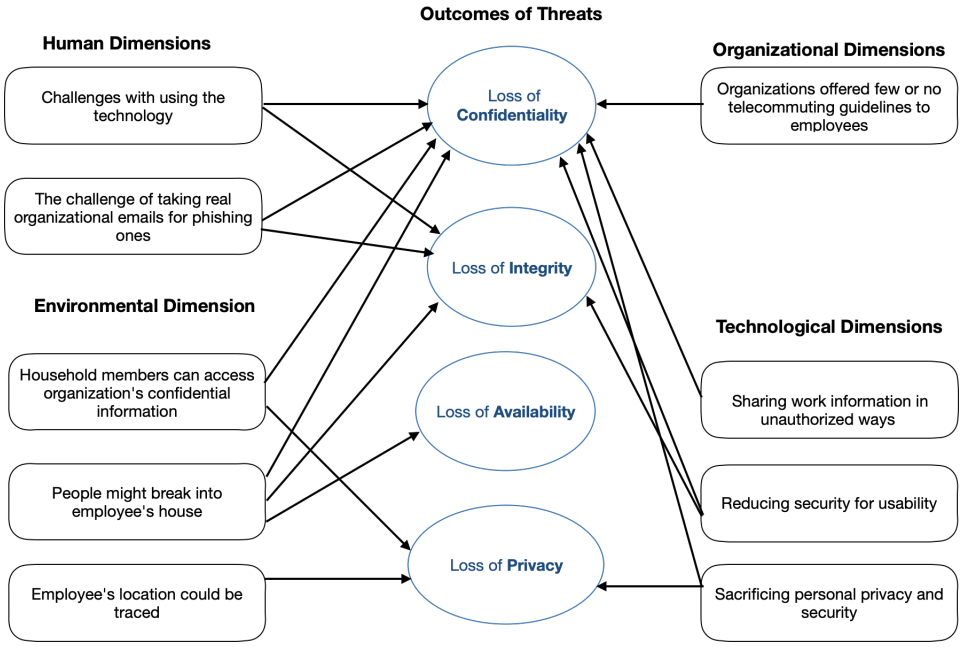

Figure 3.2: The relationship between challenges, threats, and the outcomes of threats. Arrows link challenges\threats to the outcomes of the threat.

3.6.2 General discussion

Our findings point to the security and privacy challenges, threats, and potential outcomes of threats that participants perceive while telecommuting. Figure 3.2 illustrates the consequences of a threat that could arise due to the identified challenges and threats with telecommuting, which we described in the previous section. In this section, we generalize discussion of the results in the form of perceived outcomes of threats to telecommuters and their employers. In Table 3.2 and Table 3.3, we present the challenges and threats, as perceived by participants, and show how they could lead to various outcomes of threats. We identified participants' perceived outcome of threat in which the organization's assets are at stake (Table 3.3). In contrast with office work, mass telecommuting introduces additional consequences of threats. The participants' privacy, data, and in some cases, well-being are at stake (Table 3.2). In the rest of the discussion section, we describe both types of these outcomes of threats and discuss options for mitigating some of them. It should be

noted, however, that proper evaluation of these countermeasures is subject to future research.

While some of the challenges and threats are not unique to telecommuting, the issues are amplified in scale and severity when workers solely rely on telecommuting. The severity of the challenge gets intensified due to the lack of physical proximity among coworkers for many weeks, if not months. For example, confidential information may have never been shared through unauthorized means (§3.5.2), because employees would meet in person. However, mass telecommuting takes away that opportunity, leaving employees with nothing else but to rely solely on online solutions, some of which (in isolation or in combination with other technologies) turned out to be over-restrictive or otherwise have less than acceptable usability (§3.5.2). Another example is the possibility of using technological tools to monitor employees' activities, which could result in an invasion of their privacy (§3.5.2). This challenge could lead to bigger issues, such as monitoring employees' or coworkers' daily routine even during weekends. These privacy issues became much more of a concern when long-term mass telecommuting became widespread overnight and might even remain so after the pandemic [48, 61, 172, 271]. Identifying and addressing these challenges, therefore, would go a long way toward improving telecommuting beyond the pandemic. Further, mass telecommuting could also happen in emergency situations such as power outages, earthquakes, and other natural and human-made disasters. In the rest of this section, we categorize recommendations into three types, according to the intended audience: organizations (R-O), employees (R-E), and those working with telecommuters (R-T).

3.6.3 Perceived Outcome of Threat Toward Workers

Telecommuting elevates the outcomes of threats to personal safety for employees and their households. Some participants worried that angry clients could locate their homes and terrorize them (§3.5.3). Other participants were anxious that criminals could break into their homes and steal their organizations' expensive work devices while also putting participants' privacy and safety at risk (§3.5.3). These anxieties could negatively affect employees' productivity, job satisfaction or employee retention while telecommuting [103, 205, 252]. Physical security at work

is the responsibility of the employer and is commonly implemented by monitoring and controlling access to the office space and parking lots, and by stationing security personnel in the office buildings [31, 122, 300]. In the telecommuting scenario, however, the expensive work equipment now resides in the employees' homes, and there is no physical security provided. Organizations could implement encryption of the computer's hard drive to safeguard their data [161, 183, 296, 332]. However, the safety of the employees and the household members is also at risk due to telecommuting. Therefore, telecommuting produces a negative externality [164], as it is the employer that benefits from the employee being able to telecommute, but it is the household members who have to mitigate the elevated risk to physical safety and the psychological trauma that comes with it.

Employers can put measures in place to manage the safety of the telecommuters and their households **(R-O)**. Organizations need to be sensitive to the employees' physical security and consider the reality that different employees live in neighborhoods with varying safety levels (§3.5.3). Organizations can be mindful of this threat and manage it as part of their policies or processes for handling work from home. For long-term (and full-time) telecommuting, the employers could consider setting up home alarm systems for their employees. The employers could also look into setting up work hubs where the organization's devices could be set up and the employee's safety is protected. Further, employers can educate employees about security measures at the work hub to allay their fears. We also suggest that organizations provide clear guidelines on managing the home-work environment to optimize employees' physical safety. For instance, similar to on-site organizational security measures, employers could develop processes for physical security while telecommuting, such as help lines or safety routines that employees could use if the organization's clients/customers misuse employees' personal data.

Loss of workers' privacy is the major theme that emerged in the interviews. As can be seen in the rightmost column of Table 3.2, every type of concern is related to this theme. The main reason for its omnipresence, we believe, is that telecommuting is a hybrid work situation, where employees are at home but expected to carry out the organization's activities. Therefore, employees must behave in a specific way, which comes at the cost of their privacy. For instance, employees gave clients and coworkers (and even sometimes customers) their own phone numbers

Table 3.2: Perceived outcome of threat toward workers

Asset	Employee's behavior	Threat agents	Reason for concern	Threat	Outcome of threat
1. Employee's personal phone number and home address	Employee giving coworkers their personal information to aid telecommuting	Coworkers	a. Violation of personal boundaries b. Less control over who has access to personal information	a. Coworkers could use employee's personal information for purposes other than initially declared b. Sharing of personal information without permission from the subject of the information	**a. Misuse and unauthorized sharing of shared personal data** **b. Loss of privacy** (§3.5.2)
2a. Employee's money b. Employee's privacy	Employee picking up calls from unknown numbers, not screening phone calls	Phone scammers	Reduced protection from scam calls	a. Phone scammers could obtain employee's financial information b. Increase in scam calls	**a. Abuse of personal data** **b. Becoming a victim of scams** **c. Loss of privacy** (§3.5.2)
3a. Employee's private home setting b. Housemates' privacy c. Employee's privacy	Employee forced to turn on their video camera during telecommuting	Coworkers	a. Personal environment of the employee is exposed to coworkers b. Lack of privacy in the home environment VS the work environment	a. Coworkers seeing employee's private environment and housemates b. Employee's improper disclosure of themselves	**a. Accidental disclosure** **b. Loss of privacy** (§3.5.2)
4. Employee's routine	Using technological tools that make it easy to monitor employees	Coworkers, managers	Coworkers and managers can monitor employee's activities and routine	Coworkers and managers could use this information to predict employee's routine	**Loss of privacy** (§3.5.2)
5. Employee's personal data	Giving students remote access to the employee's computer	Students	Due to a lack of computer knowledge, there is uncertainty about what students can do on the employee's laptop when given remote access via videoconferencing	Students could control the computer of a non–tech-savvy employee and access personal data	**a. Abuse of personal data** **b. Loss of privacy** (§3.5.2)
6. Employee's safety	Calling customer/client from home	Customer/client	Unmasked work phone number	An angry customer/client could locate employee's home by tracing phone calls made to the customer/client	**a. Abuse of personal data** **b. Loss of life** **c. Loss of privacy** (§3.5.3)
7. Employee's safety	Distributing care packages from home	Criminals present in neighborhood	Physical harm by intruders during a break-in to the house	Physical harm and injury	**a. Loss of life** **b. Loss of privacy** §3.5.3)

and other personal information (§3.5.2). The participants had other privacy boundaries (e.g., by answering phone calls from unknown numbers) compromised to facilitate telecommuting (§3.5.2). Workers were also worried about others taking screenshots of them without their consent during video calls (§3.5.2) and others feared that their clients and colleagues could overhear personal conversations taking place at the workers' homes (§3.5.3).

There are various ways for employers to aid their employees in maintaining privacy while working from home. Organizations can provide some form of phone number masking (which prevents others from knowing the actual phone number of the caller) or VoIP solutions [225] to employees who have to use their personal phones for work [113] **(R-O)**. Further, we suggest technology support for alerting participants of video calls when screenshots are taken, to help employees main-

Table 3.3: Perceived outcome of threat toward organizations

Asset	Employee's behavior	Threat agents	Reason for concern	Threat	Outcome of threat
1. Confidential information	Putting organizations' and customers' confidential information on social media platforms	Employees of social media platforms, cybercriminals	Lack of confidentiality on social media platforms	a. Employees of the social media platform could spy on the organization's confidential data b. Cybercriminals could exploit the vulnerabilities of social media platforms and obtain confidential information	**Loss of confidentiality** (§3.5.2)
2. Customer/client's confidential information	a. Discussing confidential information through device speakers b. Reading out clients' confidential information	Housemates	Lack of sound insulation	Housemates could overhear confidential information	**Loss of confidentiality** (§3.5.2)
3a. Citizen's information b. Political report that has not been made public	Making use of a less secure personal phone and email software	Social insiders, cybercriminals	Personal phones and email software are not configured to be as secure as work phones and emails	a. Social insiders snooping through employee's phone and accessing their text messages b. Hijacking personal email account and obtaining copies of the work emails	**Loss of confidentiality** (§3.5.2)
4. Organization's accounting information	Reducing the security of systems to aid telecommuting	Cybercriminals	Reduced security of remote desktop server	Cybercriminals could compromise the security of the system and access organization's data	**a. Loss of confidentiality** **b. Loss of integrity** (§3.5.2)
5. Confidential information	Giving students remote access to employee's personal computer	Students	Due to a lack of computer knowledge, there is uncertainty about what students can do on the employee's laptop when given remote access via videoconferencing	Student could control the computer of a no–tech-savvy employee and access confidential data	**a. Loss of confidentiality** **b. Loss of integrity** §3.5.2)
6. Client's health information	Displaying confidential information on big screens, in large font sizes, while telecommuting in the kitchen area	Housemates	Housemates could read confidential information off the screen	Housemates could view confidential health information	**Loss of confidentiality** (§3.5.3)
7. Organization's confidential information	Unable to troubleshoot work devices from home	Cybercriminals	Reduced security of work devices for telecommuting	Cybercriminals could exploit vulnerabilities in work devices	**Loss of confidentiality** (§3.5.4)
8. Organization's confidential information	Using expensive organizational work devices to aid telecommuting	Criminals present in neighborhood	Lack of physical security of work devices and recent break-in	Neighbors could break into employee's home and steal work equipment	**a. Loss of confidentiality** **b. Loss of integrity** **c. Loss of availability** (§3.5.3)

tain awareness of their privacy violations and to deter abuse of such capabilities by others (§3.5.2) **(R-E)**. To prevent clients and colleagues from hearing personal conversations happening in the household, teleconferencing software and phones could have a feature where the microphone is automatically muted when employees are not talking. Using voice recognition, the microphone automatically unmutes when the employee starts talking to the client or coworker **(R-T)**. There could also be directional microphones on phones and videoconferencing apps, whereby the technology only picks up the voice of the person in front of the computer or phone **(R-T)**.

Furthermore, there seems to be a conflict between employees maintaining their privacy and doing their job. Our findings confirm Pyöriä's work, as this author pre-

dicted disruption to privacy in employees' homes as a challenge that could arise in teleworking [264]. Our participants experienced a dilemma around whether to turn on their webcams during work meetings. For some, turning on the webcams was an invasion of privacy, as it welcomed coworkers into their private homes and lives. On the other hand, employers expected participants to always have their webcams on during work meetings as these meetings are done within work hours (§3.5.2). Further, some employees also had to give clients remote access to their personal computers while telecommuting (§3.5.2). In addition, some telecommuting solutions could aid with monitoring employees' activities and detect when employees were at or away from their desks (§3.5.2). Research shows that such online status indicators or presence sharing applications leads to privacy concerns for users [37, 64, 158, 277]. Other features of videoconferencing apps raise further concerns about employees' privacy during telecommuting. For instance, Microsoft Teams and Zoom allows meeting participants to livestream a meeting without getting consent from the participants [319, 360]. Therefore, employees' work meetings in their personal spaces can be livestreamed on Facebook Live and YouTube without the employees' knowledge. All of these situations raise questions about employers' rights over employees privacy in their own homes. Palen et al. discussed the issues surrounding privacy in a technologically connected world. Because privacy is personal, people set various boundaries in their everyday life to maintain their privacy [6, 241, 323]. However, the use of information technology disrupts or demolishes those boundaries. The authors explain the challenge further: "problems emerge when participation in the networked world is not deliberate, or when the bounds of identity definition are not within one's total control. [241]" As seen in our results, employees do not have full control over their privacy, which is a challenge. There is also the issue of context collapse in telecommuting. "The concept of context collapse describes the process by which connections from various aspects of individuals' lives become grouped together under generic terms [3, 33, 335]." Similarly, in telecommuting, workers experience context collapse and are faced with the dilemma of how to draw boundaries between their personal and professional lives. This leads to privacy issues for participants (§3.5.2).

To help create a balance between privacy and doing one's job, organizations

can have discussions and transparency on how much privacy employees are entitled to when telecommuting **(R-O)**. It may be helpful for organizations to clearly state what they expect from employees regarding having the camera on or off while working from home, dress code while telecommuting, or giving clients their personal phone numbers. There might, however, be no clear-cut answers to these questions. Moreover, they raise bigger questions that future research could look into. For example, can employees maintain their privacy while working from home? If yes, how can privacy boundaries be maintained while respecting organizational cultures, social norms, and work policies? Does the use of technologies that monitor employees' routines (mostly during work hours) violate their privacy? Should technological tools be allowed to monitor workers' activities during and after work hours when they work from home? How can employees give or withdraw their consent for recording, screenshots, or livestreaming during online work meetings without feeling stigmatized or fearing repercussions? How can organizations and technologists make sure employees are not putting their physical safety at risk when working from home (§3.5.2)? Employers and employees need to consider these different scenarios when making telecommuting arrangements.

3.6.4 Perceived Outcome of Threat Toward Organizations

The outcomes of threats related to the confidentiality and integrity of the organization's assets were the most common theme in this category (see Table 3.3). Kintner et al. and Spinellis et al.'s participants also predicted inadequate security for protecting transmitted information in teleworking as a potential challenge [174, 309]. In some cases, the organization's assets were at risk because the official work communication platforms were not usable (§3.5.2). Therefore, participants used other insecure but usable and familiar technological solutions to talk to coworkers and share clients' confidential information. Since participants no longer had the luxury of talking in person to their colleagues about work-related matters, participants were looking for technology support closest to in-person interactions. Such support made communication with coworkers easy without unnecessary setup or complicated authentication procedures (§3.5.2 & §3.5.2). Employers need to ensure that work communication platforms are very intuitive and easy, if they want to address

this issue **(R-O)**. These work communication platforms could also be linked to other popular social communication channels. For example, organizations could work toward having a secured platform on Facebook to discuss work-related information. One of the principles of secure systems design is the path of least resistance [355]. This principle states that "to the greatest extent possible, the natural way to do any task should also be the secure way [355]." Since employees are already using these social platforms anyway, employees are most likely to follow the path of least resistance. Such types of platforms are subject to future research and development.

The inability to distinguish between phishing and real emails rendered employers' announcements ineffective. Some organizations asked their employees to use their personal devices to work and expected employees to use the organization's software on those devices. Because IT personnel didn't have control or access to the employees' devices, IT personnel had to send emails to the employees with system updates required to maintain the organization's software while telecommuting. Because employees found it challenging to distinguish between fake and real emails, employees ignored important system updates sent through emails (§3.5.4). Organizations could make use of already existing solutions to digitally sign and encrypt official emails from the organizations [237] **(R-O)**. Employees would, however, need to learn and understand how these solutions work because, as previous research shows, people find it difficult to use encrypted and signed emails correctly [344]. Apart from email, we suggest that other communication platforms could be used, such as a usable official messaging platform to relate work information **(R-O)**.

There was also the outcome of threat of household members overhearing confidential work discussions. In real-life situations, these confidential conversations are mostly held in offices, which are considered safe enough for those conversations to happen. However, in the context of telecommuting, home environments do not necessarily provide sufficient sound insulation. While this might not be an acute issue for traditional households with one family, cohousing [40], collective housing, and similar arrangements that are increasingly common in urban areas where housing is expensive significantly decrease control and awareness of who might be in a household and possibly overhear discussions at any given moment.

There is no easy way to address this problem. The solution is not as simple as telling employees to take work calls where other household members cannot overhear the conversation. By default, there seems to be an assumption that the employee's home environment is a typical family setting with father, mother, and child(ren) and an office space with a closed door where the employee can conveniently take work calls. In reality, employees have a wide variety of cohabitation arrangements and environments and for some, it is simply impossible to avoid working in a space shared with housemates. Further, in some cases working in a separate room doesn't solve the problem of poor sound insulation (§3.5.3). Organizations **(R-O)** need to be sensitive to the fact that employees' living situations vary and should be mindful of the corresponding outcomes of threats to the confidentiality of work calls.

There is a need for discourse in the research community on the possible solutions to these problems. Table 3.2 and Table 3.3 present a comprehensive illustration of possible outcomes of threats to organizations and employees while telecommuting. As telecommuting becomes more full-time and long-term [48, 61, 120, 172, 212, 271], the topics and issues surrounding organizational data security and employees' safety and privacy need to be discussed and addressed. The main topic is that there is a dilemma around employees maintaining their privacy and safety while telecommuting and employers ensuring that employees carry out their work from home and safeguard their organization's data. With the increase in successful cyber-attacks on telecommuters [22, 173, 211, 346], addressing the identified security and privacy challenges and threats encountered by employees may go a long way in reducing cyber-attacks related to telecommuting. We believe our study provides insights into these challenges and serves as a basis for possible solutions to be explored and discussed and will ultimately lead to better work-from-home practices for both employees and employers.

3.7 Conclusion

Our contributions provide insights into the security and privacy gaps that exist regarding employees telecommuting and attempting to maintain their professional

Table 3.4: Summarized recommendations to organizations (R-O), employees (R-E), and those working with telecommuters (R-T)

Recommendations	R-O, R-E, R-T
1. Organizations could make use of already existing solutions to digitally sign and encrypt official emails from the organizations	R-O
2. Apart from email, we suggest that other communication platforms could be used, such as a usable official messaging platform to relate work information	R-O
3. Organizations need to be sensitive to the fact that employees live in various living conditions and mindful of the corresponding outcomes of threats to the confidentiality of work calls	R-O
4. Employers can put measures in place to manage the safety of the telecommuters and their households	R-O
5. Organizations can provide some form of phone number masking (which prevents others from knowing the actual phone number of the caller) or VoIP solutions to employees who have to use their personal phones for work	R-O
6. To help create a balance between privacy and doing one's job, organizations can have discussions and transparency on how much privacy employees are entitled to when telecommuting	R-O
7. Employers need to ensure that work communication platforms are very intuitive and easy, if they want to address this issue	R-O
8. Technology support for alerting participants of video calls when screenshots are taken, to help employees maintain awareness of their privacy violations and to deter abuse of such capabilities by others	R-E
9. To prevent clients and colleagues from hearing personal conversations happening in the household, teleconferencing software and phones could automatically mute the microphone when employees are not talking; using voice recognition, the microphone automatically unmutes when the employee starts talking	R-T
10. There could also be directional microphones on phones and videoconferencing apps, whereby the technology only picks up the voice of the person in front of the computer or phone	R-T

relationship. The COVID-19 pandemic has resulted in a trial run for mass telecommuting on a grand scale. Reports show that the global switch to telecommuting has led to an increase in cyber-attacks. We are optimistic that these insights can lead to changes in the way telecommuting is currently being carried out. These changes will be helpful during the current pandemic and other situations where employees need to telecommute, whether short or long term.

Chapter 4

Security and Privacy Challenges of Using Technological Solution to Report Sexual Assault

The goal of this chapter is that interdisciplinary innovations in human-computer interaction, privacy, and security can be used to empower survivors of sexual assault to encounter healing and justice. Our investigation into designing safe spaces online for reporting of sexual assault is a response to the clear need for confidential and accessible technological solutions that survivors of sexual assault can use to communicate their experiences in the hope of holding perpetrators accountable.

To expand the reporting options for survivors, third-party reporting centers have been put in place. Third-party reporting is when someone else reports the crime to the police on behalf of the survivor [43], who remains anonymous. Third-party reporting systems (TPRSs) allow survivors to anonymously report sexual assault to the police through a community-based support center [43, 182]. TPRS is an option used when a survivor does not want to visit a police station to make a formal police report. This option is useful for two main reasons. First, it allows survivors to record details of a perpetrator anonymously [182]. Second, when multiple survivors indicate the same perpetrator, a serial offender is identified. In this case, the police contacts the community-based support center to ask the survivor if they would consent to make a formal police report so that the police can begin a

formal investigation [43]. Many of the survivors who file a third-party report and are then approached by the third party and told that the police are interested in investigating their report follow up and file a formal report with the police [42]. The resulting filing of formal police reports has led to an increase in arrests of serial offenders [42].

Third-party reporting is, however, very limited in scope. It is currently administered on paper (P-TPRS), and there are no online systems to facilitate the reporting process, which makes the process cumbersome (for instance, survivors have to locate and visit a third-party reporting center) [43, 182]. Further, third-party reporting is also not available in all sexual assault support centers but only in a few select jurisdictions [43, 47], which defeats its purpose of increasing sexual assault reporting [182, 286]. Online third-party reporting systems (O-TPRSs) are being developed to increase the reporting choices for survivors. With an O-TPRS, survivors can, at their convenience, document their experience and offender information before submitting the report to the police. An O-TPRS could decrease barriers for vulnerable populations who do not currently have access to reporting options, and whose reporting rates are even lower than the estimated averages already cited.

Since an O-TPRS will hold sensitive information, we must address the privacy and security concerns of survivors. A considerable amount of research has been conducted on sexual assault and sexual assault survivors [34, 38, 75, 190, 287]. Some research also investigates the reporting experiences of survivors [34], including sexual assaults within the armed forces [71] and police-reported sexual assaults against youths and children [72]. However, no research has focused on survivors' concerns regarding trusting O-TPRSs. To this aim, the objective of this research is to answer these research questions:

- RQ3: What are survivors' privacy and security concerns (if any) regarding trusting O-TPRSs?
- RQ4: What could help participants trust O-TPRSs?

"Trust is the degree to which people believe in the veracity or effectiveness of a tool or system to do what it was created for and is purported to do [130]." The

act of measuring trust is used to predict whether survivors would make use of O-TPRS technology [142]. Answering these research questions, therefore, will lead to understanding what it would take for users to make use of an O-TPRS. These answers could lead to an increase in the reporting of sexual assaults.

The key contributions of this chapter are:

- We performed the first empirical study on sexual assault survivors to discover their privacy and security concerns regarding trusting an O-TPRS. We group our findings into technological and emotional (human) concerns, and we show how technological concerns can lead to emotional issues for survivors. For example, the technological concern about the *insecurity of technology* can lead to the emotional issue of *anxiety* about making an online report, the *fear of perpetrators having access to the sexual assault report*, and the *re-victimization of survivors.*

- We discovered concerns that technologists need to consider in developing O-TPRSs. For instance, on the one hand, survivors did not trust that an O-TPRS could protect their anonymity and privacy from their perpetrators and the police. On the other hand, the police did not trust that the anonymous reports sent from an O-TPRS were linked to real survivors. Technologists would, therefore, need to find a balance in how an O-TPRS can ensure both parties can trust the system.

Our contributions provide insights into concerns that survivors and support workers have about using online systems to report sexual assault in complex or unwanted relationships. We are optimistic that when O-TPRSs are designed with careful attention to users' feedback and research, such systems could increase reporting.

4.1 Background and Related Work

In its current format, a TPRS is a process or protocol to make an anonymous report of a sexual assault by a community-based support center. A TPRS is not a substitute for an emergency call, nor is it a formal police report. It is not to be used when the survivor or others are at risk of further violence. A TPRS is intended to be used

when the survivor does not want to make a formal police report but prefers to report anonymously. A TPRS is useful for the identification of offenders, especially repeat offenders.

4.1.1 P-TPRS

The P-TPR form

The current TPRS is in paper form. We describe a P-TPRS currently in use in a jurisdiction in Ontario, Canada. Page one of the P-TPRS is a cover sheet where survivors write their personal information. On pages two and three, survivors describe the offender and the offense (see Appendix A.1 for the questions asked on a sample P-TPR form.)

The P-TPR process

The survivor goes to a community-based center to carry out the P-TPRS process. The community-based center, which is usually a hospital or a sexual assault support center, is the third party. The survivor meets with a representative, either a nurse or a social worker, at the third-party reporting center. If the survivor is not willing to make a formal police report at this time, the representative at the center can provide the option of filling out a third-party report form. The survivor has to fill out the form at the center and return it to the representative before leaving the center. If the survivor doesn't feel capable of filling out the form by themselves, the representative can listen to the survivor's story and fill out the form with the survivor's consent. Afterward, the representative de-identifies the form by removing the cover sheet. The representative sends the de-identified P-TPR form to the police. However, the hospital or the sexual assault support center, which is the third party, maintains the identity of the survivor. The police receive the content of the form and enter it into a database, making it easier to identify serial offenders [43].

A serial offender is identified if at least three people accuse the same person of sexual assault. If a serial offender or a trend is identified, or if the police believe the survivor is in imminent danger, the police can contact the community-based center. The center can reach out to the survivor to see if the survivor is willing to

take further part in the investigation or even if they might consider changing their report from an anonymous report to a formal police report [43]. Figure 4.1 shows the P-TPR process.

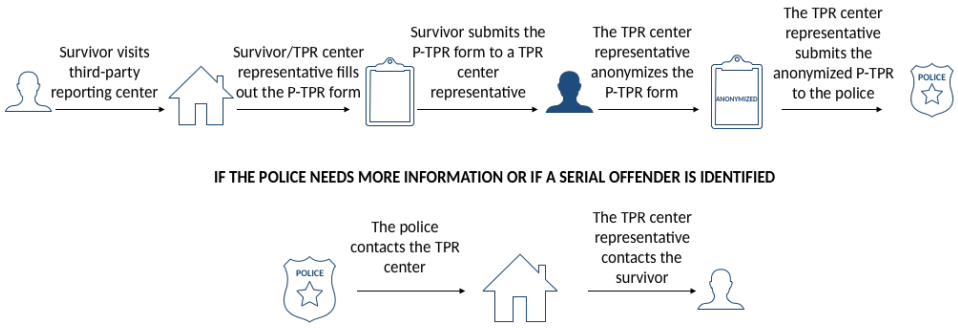

Figure 4.1: P-TPR process

4.1.2 O-TPRS

The O-TPRS supports the goal of reducing barriers to reporting by providing survivors with a new way to report that is anonymous and does not require visiting a community-based center. It also streamlines the third-party reporting process by removing the human involved in the P-TPRS.

The O-TPR form

The O-TPR form works similarly to the P-TPR form. We provide the description of an O-TPRS being developed by VESTA Social Innovation Technologies (Vesta) [333]. The O-TPRS includes a cover page and pages to type out information about the survivor, offender, and the offense (see Appendix A.2 for a sample of an O-TPRS prototype).

The O-TPRS process

The survivor fills out the TPR form online. The O-TPRS, which could be an app or a website, is the third party. The survivor can download the O-TPRS app from the app store or can use the website version. Unlike the P-TPR form, the O-TPR provides unlimited space for the survivor to type out their experience. The survivor

fills out their information, and they can save and review the information before submitting it. Before the form gets sent to the police, the O-TPRS automatically de-identifies the form. The O-TPRS, which is the third party, maintains the identity of the survivor. The police enter the content of the de-identified form into a database, making it easier to identify serial offenders. If a serial offender or a trend is identified, or if the police believe the survivor is in imminent danger, the police can contact the O-TPRS. The O-TPRS then reaches out to the survivor to see if the survivor is willing to take further part in the investigation or even if they might consider changing their report from an anonymous report to a formal police report.

O-TPRSs are not widely available. However, several organizations are looking into deploying O-TPRSs. For instance, Vesta has developed an experimental version of an O-TPRS, which is being deployed to various sexual assault centers to pilot the program. Figure 4.2 shows the O-TPRS process.

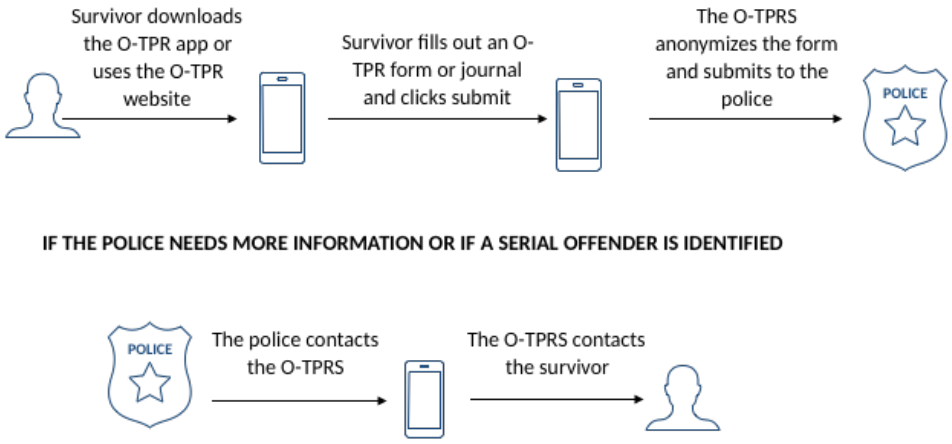

Figure 4.2: O-TPR process

4.1.3 Trust and technology

Research has been done on the concept of trust and technology usage. McKnight et al. define trust in technology as "belief that a specific technology has the attributes necessary to perform as expected in a given situation in which negative consequences are possible [207]." Prior work shows that heightened levels of trust are associated with heightened levels of intended use [115]. Trust in technology is

used to predict the intended or actual adoption of technology [353]. It is also connected to appropriate and inappropriate use of technology [219] and technology over- and under-reliance [13].

Many works on technology and trust exist. Hardre, for instance, studied when, how, and why people trust technology too much [130]. Hardre analyzed various scenarios of everyday technology use where users tend to trust technology. Some of these scenarios include massive breaches of banking systems, even though people believed that these systems would keep their financial information safe [130].

Minimal research has been done on how survivors build trust in sexual assault technology. Work by Liu is closest to ours [189]. Liu discussed issues that sexual assault prevention (such as the Circle of 6 app) and reporting technologies (such as the I've-Been-Violated app) may have in the future. The author evaluated these apps using the US Federal Trade Commission's fair information practice principles (FIPPs). Based on these principles, the author predicted that the following concerns could arise with using the apps: false allegations, security issues with the internet, fears of lack of anonymity, insensitivity to survivors' experience, lack of clarity on collected information, and lack of user-friendliness.

Our contributions are as follows: 1. We performed the first empirical study with survivors and sexual assault support workers to identify issues related to trusting O-TPRSs. 2. In addition to corroborating concerns of Liu [189] that technology could be used to make false allegations, we identify additional concerns with trusting O-TPRSs, such as the dual use of technology in not only reporting but also aiding sexual assault. 3. Further, we uncover the relationships between these concerns and discuss the issues related with designing an O-TPRS.

4.2 Methodology

4.2.1 Data Collection

We recruited participants using three methods and specific eligibility criteria. First, we used word of mouth in the professional network of one of the authors, who had extensive contacts with the workers and administration of sexual assault centers. Second, after we presented our study to an association of sexual assault centers

in the Province of Ontario, its members distributed our recruitment notice to their clients, some of whom were in support groups. Third, we used snowballing with the help of already recruited participants. To be eligible to take part in the study, participants had to be 19 years old or above. Further, participants had to be survivors of sexual assault, support workers, or both. We defined support workers as those who supported survivors throughout the process of reporting sexual assault. Support workers included volunteers and staff of sexual assault report centers and the police. We recruited both survivors and support workers because both parties are involved in the TPRS process. None of the recruited participants had prior knowledge of TPRS. We recruited participants who had no prior knowledge of TPRS to get an unbiased view of both the paper and the online version of TPRS.

We piloted our study procedure with three participants—one participant for an interview session and two participants for a focus group session. In the interview pilot study, we asked the participant about her thoughts regarding O-TPRS. We realized that it was difficult for the participant to imagine how an O-TPRS would look and function. Based on this result, we made a video showing an O-TPRS prototype (see Appendix A.2 for pictures of the prototype). We showed participants this video to illustrate an O-TPRS and to help participants understand how an O-TPRS would function. We chose to use a video for three reasons. First, for interview and focus group sessions facilitated through online video calls, we found a video more effective than a verbal explanation. Second, using a video provided a consistent explanation of the user interface across all sessions. Finally, the use of a video helped to fit each session into one hour. We piloted this approach in the pilot focus group, and we discovered that the participants could understand the O-TPRS better. We therefore used this approach for the main study. Apart from this change, all other procedures in the pilot interview and focus group were the same as those used in the main study. After adjusting the study design based on the outcomes of the pilots, we recruited participants for the main study.

We used multiple qualitative research methods [220, 349]. As suggested by Hammarberg et al. [128] and illustrated by Willis [349], using various data collection methods helps to provide better insights for sensitive research topics. We conducted semi-structured individual interviews and focus groups with participants [220]. Because of the sensitivity of the research, we gave participants the

option to decide whether they were more comfortable having a semi-structured interview or participating in a focus group. For our interviews, we chose a semi-structured style to allow participants to express their thoughts in their own way and add information as they saw fit, without the restriction of a structured interview [65]. We also offered focus groups because focus groups allow participants to discuss sensitive or controversial topics in a group setting [220]. Due to participants' shared experience, sometimes focus groups "reveal aspects of experiences and perspectives that would not be as accessible without group interaction [220]," which leads to a better quality of data on sensitive topics [220].

We conducted in-person or video interviews and focus groups, based on the participants' preference, at the participants' preferred location. Some of these locations included the participants' home or a sexual assault support center. We conducted video calls via Skype or Zoom. To protect participants' privacy, online sessions were audio recorded not using Skype or Zoom but locally on a laptop. Collected data is stored on a disk encrypted with 256-bit AES seeded with a 22-character random password. Participants were compensated with $20, paid in person or sent via e-transfer. For in-person interviews, sexual assault social workers were present to provide support to participants if needed. We sent online support materials that were created by sexual assault centers to the participants that we interviewed via video call. All focus groups were held at sexual assault support centers, either by using existing support groups or by forming focus groups for interested support workers at the centers. Participants in both online and in-person focus groups were physically present in the support centers, and sexual assault social workers were available to provide support. The social workers were compensated by their support centers, as focus groups took place during their regular work hours. We conducted seven interview sessions and five focus groups via video calls, with the rest (one interview and focus group) in person. Our institution's Research Ethics Board approved the research before any data collection took place.

We wanted to conduct separate focus groups for survivors and support workers. However, during the focus groups for support workers, some support workers self-identified as survivors. Further, when we collected participant demographics for the survivors' focus groups, we discovered that some survivors were also support

workers. During data analysis, we realized that the responses from survivors and support workers were similar; therefore, distinguishing between the two groups was unnecessary. Table 4.1 shows participants who self-identified as survivors.

4.3 Participants' Demographics

4.3.1 Interview and focus group procedure

We proceeded with the interviews and focus groups after the participants gave informed consent to participate in the study. We assigned pseudonyms to participants and asked for their demographic information. Though we asked participants about sensitive issues, we did not ask them to disclose any sensitive information that they did not feel comfortable sharing. We reminded participants that they could skip questions they did not feel comfortable answering. During each session, we explained the meaning of P-TPRS, showed participants a copy of the P-TPR form described in Section 4.1.1, and asked participants their thoughts on using the P-TPRS to report sexual assault. Afterward, we played a video that explained the O-TPRS (see Section 4.1.2 for an explanation of the O-TPRS that was shown to participants). We then asked participants their thoughts on using the O-TPRS to report sexual assault.

To avoid priming participants, we asked participants their thoughts on using both systems rather than asking just about O-TPRS. We also asked participants what would make them comfortable using each system. We assured participants that there were no right or wrong answers, and participants could skip questions they did not feel comfortable answering.

We conducted online focus groups and interviews via Skype or Zoom based on participants' preference. For online interviews, participants chose a quiet and private location convenient for them. For the online focus group, the participants gathered at their preferred sexual assault center meeting room, and the researcher called in to conduct the focus group. We chose this arrangement because it allowed participants to get support from social workers present at the center if needed. We used focus groups and interviews because literature suggests that vulnerable populations participate better in data collection when they are given multiple choices [98]. Fur-

ID	Age	Gender	Survivor/Support Worker	Interview/Focus Group	Educational Level
P1	36	M	SW	I	Bachelor's
P2	63	F	SR	F	Bachelor's
P3	48	F	SR	F	College
P4	33	F	SWSR	F	Bachelor's
P5	67	F	SR	F	Bachelor's
P6	80	F	SR	F	College
P7	36	F	SWSR	F	College
P8	74	F	SR	F	High school
P9	60	F	SR	F	High school
P10	25	F	SWSR	I	College
P11	44	F	SW	I	Master's
P12	52	F	SWSR	F	MBA
P13	27	F	SR	F	High school
P14	22	F	SR	F	High school
P15	24	F	SWSR	I	Master's
P16	19	F	SR	F	High school
P17	19	F	SR	F	High school
P18	47	F	SWSR	F	College
P19	46	F	SWSR	F	Bachelor's
P20	20	F	SWSR	F	College
P21	63	F	SWSR	F	Bachelor's
P22	21	F	SWSR	I	College
P23	31	F	SR	I	College
P24	19	F	SWSR	F	Bachelor's
P25	29	F	SWSR	F	Bachelor's
P26	39	F	SW	F	Bachelor's
P27	51	M	SW	I	Bachelor's
P28	51	F	SWSR	I	College
P29	26	F	SW	F	Bachelor's
P30	37	F	SW	F	College
P31	62	F	SW	F	College
P32	35	F	SW	F	Master's
P33	22	F	SW	F	High school
P34	49	F	SW	F	Bachelor's
P35	26	F	SW	F	Bachelor's

Table 4.1: Demographics of participants. SR, SW, I, and F represent survivor, support worker, interview, and focus group, respectively.

ther, online focus groups have been found to be useful for reaching members of hard-to-reach populations [105]. Underhill and Olmsted [326] showed that there was no difference between the quality and quantity of data obtained in face-to-face and online focus groups.

Afterward, we compensated the participants. One researcher took part in each interview session. All interview sessions were audio recorded.

4.3.2 Data analysis

We transcribed and coded more than 12 hours of recorded interviews and focus group sessions, each an average of 55 minutes long. We analyzed interviews using thematic analysis [126], a "set of procedures designed to identify and examine themes from textual data in a way that is transparent and credible [125]." We followed the data analysis steps outlined by Guest et al. [125].

One researcher segmented and coded the transcribed interviews into categories and types. Two researchers discussed the relationships that developed from the codebook. Afterward, two researchers identified the themes that emerged from the data. We conducted data analysis concurrently with the data collection and reached theoretical saturation after 34 interviews and focus group sessions, as no new codes emerged from the last data collection session. Figure 4.3.2 shows the saturation graph depicting the total number of codes after each interview.

4.3.3 Participants

We recruited 35 participants (33 women and 2 men), aged 19 to 80 years (the mean age was 40 and median was 36). Table 4.1 provides the demographics of the participants. Participants' occupations included counselor, police officer, daycare worker, cook, barista, event planner, social worker, baker, frontline worker, stay-at-home mother, and student. All participants were survivors, support workers, or both.

4.4 Results

To better understand survivors' concerns regarding trusting an O-TPRS, we grouped our findings into **technological** and **emotional** concerns. We define *technological*

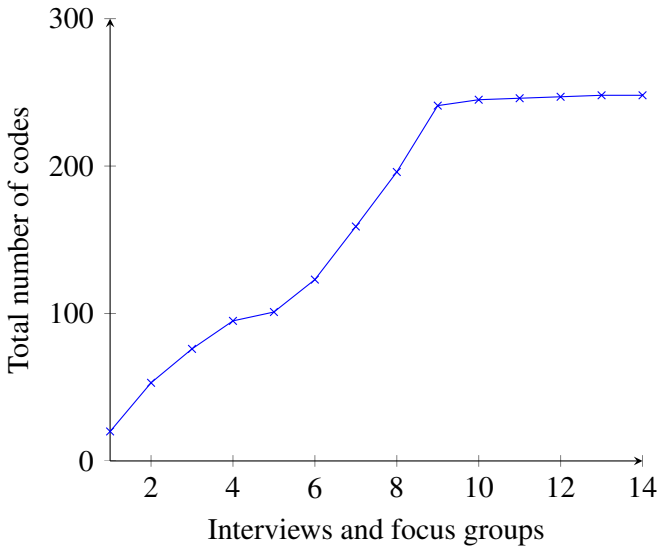

Figure 4.3: Number of codes after interviewing each participant

concerns as the issues participants had with using an O-TPRS to report sexual assault. We define *emotional* concerns as the psychological issues participants had with using O-TPRS. Most of the *emotional* concerns are related to issues with the *technology* of the O-TPRS. In the next sections, we illustrate these concerns and explain how the concerns are related. To provide more context, in the rest of the chapter, we use SW, SR, and SWSR along with participants' ID to indicate if participants are support workers, survivors, or both respectively.

4.4.1 Technological concerns

The insecurity of technology

The insecurity of technology was a concern. Participants found it challenging to trust that the technology would be safe to use in reporting sexual assault incidents. P8-SR, for instance, remarked: *"I wouldn't feel comfortable at all [using an O-TPRS]. I have zero confidence in online. Although I [use the] computer [and], I know the computer, ... I don't know it like hackers do. So, therefore, I would not put any of my information [into an O-TPRS]."*

When comparing the submission of a TPR form through a human versus through an online platform, participants trusted humans more. P5-SR, for example, commented: *"I still see [the] human factor is [a] dominant form of communication rather than technology, which can be twisted and broken and is not secured ... Technology to me is not safe because there are so many ways to hack it."*

Because of news of past data breaches, participants assumed that a breach would also happen with an O-TPRS. P6-SR, for instance, remarked on past data breaches: *"[Technology is not] safe. I don't care who says it is; it isn't. [You] just have to listen to the news. The banks have been hacked ... the government's been hacked ... Everybody else [has been hacked]."*

The lack of trust in the internet's security also led to the fear of survivors' losing their confidentiality and privacy. Because of this fear, participants limited the amount of personal information that they shared online. P20-SWSR explained: *"I personally don't put or do anything on the internet that I'm going to be upset about anyone knowing. If I don't want people to see pictures of me with less clothes on, I probably just should not post those. ... So I don't know how I would trust [an O-TPRS] with something that I would be upset about someone seeing."* In their research on trust in e-commerce technology, Araujo and Araujo [9] note that the fear of lack of information privacy is associated with a distrust of technology.

The insecurity of technology led to **anxiety** about using technology to report sexual assault. P7-SWSR, for instance, explained how the use of technology could lead to anxiety: *"I would prefer a paper [TPR] because places that are supposed to be totally secure are being breached. ... And [using technology to report] would give me more anxiety than necessary."* P29-SW also explained: *"[The thought of using an O-TPRS] makes me nervous ... it's kind of like a fear of [the] unknown. I know that going into the [police] station is a lot more vulnerable too, but I have confidence that confidentiality is kept in place due to their legal obligations. I don't fully agree that when things are online that it's completely confidential."*

The possibility of hackers accessing an O-TPRS also leads to **the fear that perpetrators** [235] could see the O-TPR details. Access to such information by the perpetrator could lead to the **re-victimization of the survivor.** P16-SR explained this fear: *"Servers get hacked, and people can see that information. And sometimes there's not anything that you can do to stop that [from happening.]*

That's what skews me. [Your sexual assault information] can get into the hands of the wrong person."

Lack of competency with using technology

Unfamiliarity with using any form of technology was another reason participants were not keen on trusting technology. P10-SWSR explained this challenge: *"I wouldn't be comfortable [using an O-TPRS] just because I'm not really comfortable with technology, so I don't see myself downloading a [TPR] app. ... Just when I [decide to report], I would not think of [using] something I am not comfortable with."*

Lack of anonymity assurance

According to participants, with O-TPRS, there was no assurance of anonymity of their personal information. Participants needed a guarantee that the information submitted through an O-TPRS would remain anonymous. They compared the anonymity a P-TPRS provided to that of an O-TPRS. In the P-TPRS, the third-party center representative takes off the cover sheet and sends the anonymized TPR to the police (see Section 4.1.1 for how the P-TPRS works). Though the O-TPRS also promises the same level of anonymity, participants found it hard to believe that their report would be anonymized. P22-SWSR explained this concern: *"If I go to a hospital and [I] fill out [a P-TPRS], [the nurses] can remove the cover sheet and then give [the anonymized P-TPRS] to the police ... something about that [process] feels safer [than an O-TPRS]. ... If I didn't have to [put] my own information [online] when making a report, then that would be better."*

The traceability of online reporting

There were concerns about the traceability of activities carried out on the internet. Participants believed that activities done on the internet left a lot of traces. Further, participants feared that sensitive sexual assault information submitted online could be traced back to them. P16-SR explained this problem: *"I would be scared to use an app or a website [as an O-TPRS] because ... once [the sexual assault information] is on the internet, it's on the internet. ... Even if you deleted the app,*

and then [people] go through your iCloud history you can see all the app that's uninstalled and installed. There's a lot of trail that can be traced back [to you] and that would be my number-one concern."

Participants compared the traceability problem of an O-TPRS to the P-TPRS. P3-SR, for instance, stated: *"I know everything can be traced, so if I send [the sexual assault information online] to the people that are supposedly the third party, that are keeping my confidentiality, there's still a trace somehow. But if I write this down [on a P-TPRS], and I hand in this paper, there's no trace at all."*

This concern was associated with **the fear that perpetrators could see the O-TPRS.** This *emotional concern* was prominent in the scenarios where the survivors knew the offenders. P22-SWSR explained this challenge: *"In my situation, I know the person that [assaulted me]. It's someone that I see from time to time. If there's some way for the offender to access this [online] form and then [the offender] can check the IP address that it was sent from and then it gets tied back to me, then I'm worried that there's going to be some ... kind of revenge. ... I [have the] fear that somehow [the online report is] going to be tied back to me. And then the person that did [the sexual assault] is going to know [and] get mad."* The issue also leads to the **re-victimization of the survivor.**

The dual use of technology

It was sometimes hard for participants to come to terms with the fact that the technology that is used to aid sexual assault or harassment could be used to reduce the occurrence of such crimes. This challenge sometimes made it difficult for survivors to trust the use of technology in reporting sexual assault: *"[Using technology to reduce sexual assault] is almost like an oxymoron. Because all we hear about is the sexual violence on the internet and people accessing porn on the internet and not as much of the reporting piece and safety."* (P18-SWSR). This disbelief of the participants was understandable, given how much sexual violence is technology facilitated [145, 148–150, 258].

The possibility of false reporting through O-TPRS

An O-TPRS could be misused. A person could submit a false online sexual assault report, or could submit multiple times, thereby reducing the credibility of the platform. Regarding this possibility, P11-SW remarked: *"I could see people wanting a certain level of reassurance that someone didn't just go on [the O-TPRS] and, because they were mad at their ex or something, [submit an O-TPR form]."* This problem was a major concern for the police. P1-SW, who is a police officer, explained: *"I'd be afraid of people misusing [the O-TPRS], either as a prank, kids playing a joke on somebody, or even for malicious reasons. If someone was out to get somebody else, then they could make this [online] third-party report. And if it would go to the police and be reported in the police databank, then there wouldn't really be any other corroborating information, it would just be sort of that mark on the database."* Regarding the possibility of such pranks happening with a P-TPRS, P1-SW commented: *"It's harder to lie to another person than it is on the computer."* While Liu [189] predicted the possibility of false allegations when using technology to report sexual assault, our findings provide empirical evidence that Liu's concerns are shared by TPRS stakeholders.

Lack of trust in apps compared to websites

The type of technology used for the O-TPRS influenced participants' decision to trust the system. Participants were more willing to trust websites than smartphone apps because they believed websites were a more secure option. For instance, P14-SR explained why she would rather use a website: *"Apps are still so new on so many levels, it's so easy to get an app with just one tiny little bug in it and that's [the attacker's] entryway to take all your information."*

Further, participants associated the use of apps with unserious use cases or activities. P34-SW explained: *"My only concern is when I think of an app I tend to think of it as something fun, almost enjoyable ... [For instance, you can say] 'Oh, I have an app to go grocery shopping,' 'Oh I have an app to do my banking,' 'Oh, I have an app to report my sexual assault ...' You see what I mean? [Reporting through an app] takes away a little bit of that seriousness. [It takes away] the severity of [the sexual assault]. So that disturbs me. Whereas [using a website] you*

can do many different things online. [A website] just seems a bit more appropriate." For P33-SW, her mental model regarding apps was geared towards using apps for fun activities.

Sometimes using an O-TPRS (either an app or a website) reduced the seriousness of the crime. P10-SWSR explained this concern: *"Reporting sexual assault online could be ... a de-sensitive experience. Currently, you report online for things like breaking into your car. I just feel like the severity of a human right violation being able to be typed [online] maybe can minimize someone's experience."*

Since apps are mostly used on phones, participants were concerned that the safety of the information on the app depends on keeping the phone safe. P14-SR expressed this concern while explaining why she would not use an app: *"[My sexual assault information] is not a personal information I want [on] my phone [because my phone] can be taken from me. ... It just takes one minute for someone to creep your phone, or your phone didn't lock right, or doesn't have a lock. Somebody can hack your phone because you read a [malicious] email on your phone. [For a website, the hackers] have to go directly for the website."* For P14-SR, a compromise of her phone security also meant a compromise of the app.

Using a phone to access the O-TPRS (either through a website or an app) could lead to **unauthorized people having access to the sexual assault information.** If someone sees the information on the phone, that information is no longer anonymous. Such a person could be one's partner or child, or even the perpetrator. P16-SR explained: *"If you had a partner, and they went through your phone and they saw that you had [O-TPRS] opened on your browser or app, and then they go through [the saved report] ... some people live in not so great relationships where there is not a lot [of] trust ... That can put [the survivor] in danger. That's scary for me [because] some women don't have that option to keep their phone."* If it is the perpetrator who stumbles on this information, this could lead to **re-victimization of the survivor**.

Further, participants thought that seeing an app about sexual assault on one's phone could lead to a survivor's **reliving the experience through constantly seeing the app**. P14-SR explained this *emotional concern*: *"I don't want an app on my phone about my experience. Every time I see it, I am going to think of [the sexual assault incident]."* P10-SWSR further stated: *"Anytime you open your phone,*

you might see the app and then you just remember that you were assaulted and you have to finish this [sexual assault] application." The presence of the app on the phone would be a constant reminder to survivors that the sexual assault took place.

The misuse of personal information for targeted advertisement

Information kept online can be misused by the O-TPRS. Because of the common practice of marketers using online information to serve ads, participants were concerned that the O-TPRS could use their personal information for ads. P26-SW expressed this concern and remarked: *"[If the O-TPRS is using my information for ads] I think that's where I would lose comfort in online [TPRS]. [The knowledge] that [my sexual assault information] is somewhere, as a data point to me, and then, suddenly my ads are coming up with 'take self-defense courses,' 'wear modest clothes,' or something. ... I would lose comfort in [the O-TPRS] for sure."*

Lack of control

Participants believed they were more in control when they used P-TPRS. There were concerns because of the errors that could occur when using technology, and participants believed they had no control over any of these errors. P25-SWSR expressed this concern in comparison with P-TPRS: *"If you're sending [a sexual assault report] online, there's always room for technology error [or] the form not going through properly. However, if a person is supported by a counselor or ... [a sexual assault support] agency in doing this, there can be some follow-up by that counselor with the police to say, 'Hey, did you get this third-party report?' ... just to confirm that [the police] did receive [the O-TPR form]."*

Concerns about the unlimited input in UI

While there were many user interface concerns, we report only the concern over *unlimited input*, which appears to have privacy and security repercussions. The information provided by the survivor because of unlimited input could lead to **re-victimization of the survivor** through court proceedings. The O-TPRS provides survivors with unlimited document space and time to type details about the sexual assault incident (see Section 4.1.2 on how O-TPRS works). However, this for-

mat could lead to issues for survivors. P11-SW explained this concern: *"I worry about [the survivor's] inner thoughts being documented in a way that could be used against them in real life. [For instance,] if I was assaulted at 3 [am] and I'd been drugged ... and I thought I had this [O-TPRS], I'm [going to] get this information in right away ... and then I hit send. Nobody else is [there to say], 'Hey, maybe, you need care right now. You need to be [in a] more grounded [291] place before you actually press send.' ... Having some guidance to say, 'You know, the police will ... understand you better when you're in a different spot.' That's my only [concern], because I worry about that information becoming part of some legal document or the public record. I've seen in court how words and things can be spun [against the survivor]."*

P21-SWSR explains this issue further: *"[The input in the O-TPRS] could be used against [the survivor] in a court of law [since the O-TPRS allows survivors] to be adding to [the O-TPR form] for several months after the assault. ... [For instance, you] get a survivor who's at home, feeling bad, and ... she's [going to write] something really horrible blaming herself. [She could say,] 'If I hadn't been at the bar, nothing would have happened,' 'I should kill myself, maybe ... I'll take the children with me' ... and those are the sorts of things women say or think in the middle of the night. But in the depths of depression, that might spill out. And then if this becomes a court case, the defense attorney gets hold of that and he's going say, 'Well look even here, you said it was your fault.' ... I think if people can talk about things over the course of months, it's going to be more [of an] opinion and feeling than factual. And that scares me [about O-TPRS]."*

4.4.2 Emotional concerns

Various emotional concerns are related to technological concerns. These emotional concerns are *anxiety, fear of perpetrators seeing the O-TPRS, re-victimization of survivors, unauthorized people having access to the sexual assault information, and reliving the experience through constantly seeing the app*. We discussed these concerns in previous sections. In this section, we discuss emotional concerns that have not previously been addressed.

Lack of human support

Having no human interaction was a major reason participants were not comfortable to trust and use an O-TPRS. Participants believed that online systems lacked empathy, which made it difficult to trust an O-TPRS fully. P15-SWSR highlighted this concern: *"It's draining to fill out [your sexual assault story] on a[n] [online] form rather than conveying the story to a person. ... At least with people, they can [express] empathy, or it's like you're telling it to a person versus a computer screen ... [that's] like talking to a wall."*

In some cases, not having human interaction can lead to **re-traumatization for the survivors.** P25-SWSR, for example, remarked: *"I think that this [online] form can be traumatizing for people trying to fill this out on their own. ... Just having a support person near them, even if they're not helping them to fill out the form, but they're close by so that if grounding [291] or some crisis support is necessary, there's someone around to do that with that person."*

Human support could be in various forms. Some participants were open to having an online audio or video form of support while filling out an O-TPRS. P22-SWSR explained that *"Having the option on the [O-TPRS] to be able to chat or to call somebody will be great. ... At times like that, questions can be very confusing ... you're disoriented and traumatized and it can be really hard. So knowing that somebody can walk you through it if you're not face to face with somebody ... [that] would be a great asset."* Other participants, however, believed that nothing could replace face-to-face human support. P8-SR, for instance, commented: *"[An O-TPRS is] missing the human link. You need the human link. The one thing that really works is the fact that you're face-to-face with a real person who's exhibiting empathy towards you and is concerned about you and would help you overcome what happened to you. ... I like walking into a place and seeing this empathetic face and then having someone offer me [a tissue] if I'm going to lose it."*

Having no human in the loop

Having a human in the loop was important to prove the legitimacy of the report. Participants who were police officers were concerned about trusting anonymous reports if there was no human involved. P1-SW, for instance, stated: *"An O-TPRS*

[doesn't have] either the check of a nurse or counselor or something from the social work side. ... Generally when someone's telling a nurse or a counselor something, I put more weight on that as opposed to just an anonymous [report that someone] typed out on their computer and sent it in. ... It's just easier for me to put weight behind it if [the survivor has] actually gone through and spoken to a person face-to-face as opposed to just over the internet."

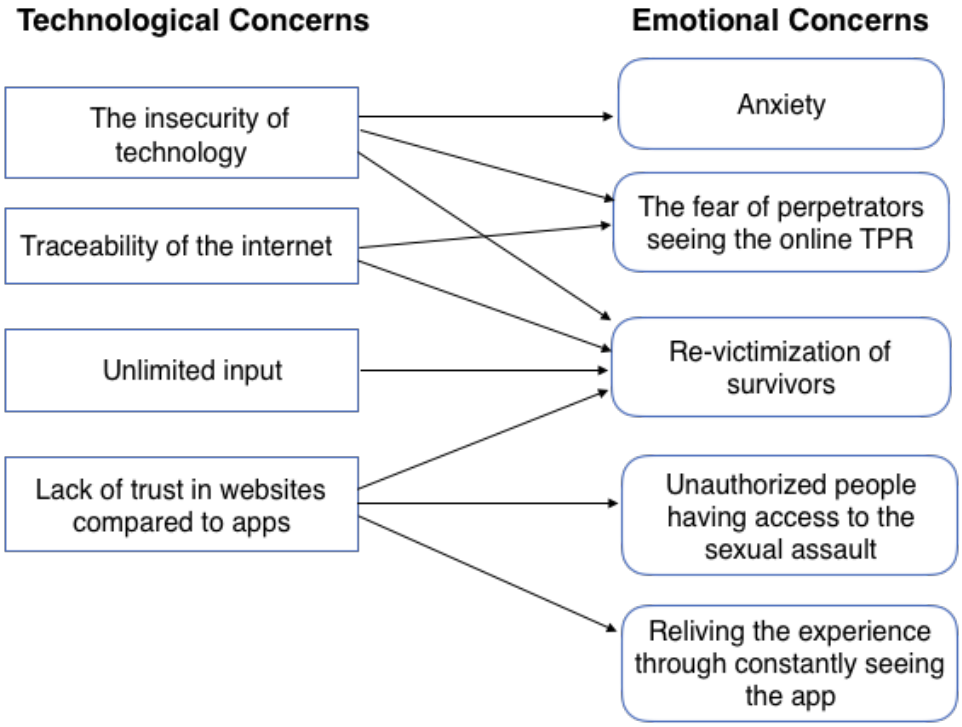

Figure 4.4: The relationship between technological and emotional concerns

4.5 Discussion

4.5.1 Limitations

Our sample could have been more balanced and diverse. It had more female (86%) participants, though statistics show that more women experience sexual assault [236, 306]. Most of the participants (86%) were also recruited through sexual

assault centers. In addition, the involvement of more than one researcher in the data collection and initial coding would have reduced personal bias. Furthermore, as with any interviews and focus groups, the data were self-reported and may have been affected by a number of systematic biases such as halo effect, social desirability, and acquiescence response bias [79]. Nonetheless, we believe that the results of our study can serve as a basis for further research on how O-TPRSs can be designed to support survivors of sexual assault.

4.5.2 Survivors vs. police: balancing their needs

For the sake of clarity, we define privacy and anonymity. Anonymity can be seen as a type of privacy. Privacy and anonymity are related but can be differentiated in some contexts. Webb [340] defines online privacy as the ability to "control who (if anyone) sees what activities you engage in online. In other words, 'they' can see who you are, but not what information or websites you access or seek." The author further defines anonymity as, "when you opt to have your online actions seen, but keep your identity hidden. [This means that] 'they' can see what you do, but not who you are." In line with Webb, we define privacy in an O-TPRS as the ability of the survivor to control who can see that the survivor used an O-TPRS. We define anonymity as the ability of the survivor to make sure that others cannot learn that the survivor has used an O-TPRS, even though others might know that someone used the system. Privacy means knowing a O-TPRS user's *identity* but *not* their *actions* in the system. Anonymity means knowing the *actions* of a user in the O-TPRS system but *not* the user's *identity*. Table 4.2 illustrates these definitions.

	Know my actions	**Do not know my actions**
Know my identity	No privacy and no anonymity	Privacy but no anonymity
Do not know my identity	Anonymity but no privacy	Privacy and anonymity

Table 4.2: Privacy and anonymity of survivors in an O-TPRS.

To understand how privacy and anonymity relate to our findings, we make the following definitions. We define *identity* as a survivor. We define *action* as using an O-TPRS. We define the actors as the perpetrator, the police, or family and friends that the survivor has chosen not to disclose their sexual assault experience

to (assuming the perpetrator doesn't fall into the latter category).

Our findings suggest that the O-TPRS should provide these properties:

Privacy protection from the perpetrator: Even though the *perpetrator* knows the person is a *survivor*, the *perpetrator* must not know that the survivor is using or has used an *O-TPRS*. (See examples in Sections 4.4.1, 4.4.1, 4.4.1, and 4.4.1.)

Anonymity protection from the police: The *police* must not know who the *survivor* is, while the *police* know that a "survivor" filled out an *O-TPRS report.* (See examples in Section 4.4.1.)

Privacy and anonymity protection from others: The survivor's *family and friends* must not know that the person has experienced a sexual assault. In addition, the *family and friends* also must not know that the person used or is using an *O-TPRS.* (See examples in Sections 4.4.1, 4.4.1, 4.4.1, and 4.4.1.)

Because both privacy and anonymity are related, a compromise of one could lead to the compromise of the other. There are many concerns that need to be addressed in designing an O-TPRS. When using an O-TPRS, the anonymous reporting of sexual assault is completed after a survivor submits an O-TPR form to the police (see Figure 4.2). The two main actors in the O-TPRS are the survivor and the police. The survivor must trust that the O-TPRS has anonymized the O-TPR form before sending it to the police. However, our results suggest that survivors find it difficult to trust that the O-TPRS can preserve their privacy and anonymity (for instance see Sections 4.4.1 and 4.4.1). The police must also trust that the report received from the system is not a false allegation. The police find it challenging to trust that the anonymous reports from the O-TPRS are from survivors (see Section 4.4.2). Therefore, survivors' need for privacy and anonymity is pitted against the police's (1) need to know the identity of the survivor and (2) the concern that anonymity could increase false reporting. The challenge for the O-TPRS designers is that without finding a solution that can satisfy these two stakeholders, it is unlikely that either will trust an O-TPRS. We discuss these concerns in depth in the following sections and explain how they affect survivors and the police.

4.5.3 Trust of survivors in an O-TPRS

Before sending the O-TPR form to the police

An O-TPRS requires both privacy and anonymity. Survivors want to send anonymous reports to the police. That means that the police should be able to identify that they have received a report from a survivor without being able to trace the report to the person who submitted it. Survivors also want to maintain their privacy by having control over who sees that they are using an O-TPRS.

The survivor should be able to trust that unauthorized people will not discover that the survivor is using or has ever used an O-TPRS. The O-TPRS has to be designed so it is not obvious on the survivor's device. Further, it should be unknown to the perpetrator that the O-TPRS will report sexual assault. This requirement could be achieved by using a pseudonym for the O-TPRS app or website; however, this design could lead to usability issues for the survivors because survivors would have to remember the pseudonym for the app.

Several proposals for addressing this problem have been put forward. For instance, for survivors of domestic violence, Arief et al. [11] suggest the design of an app that could automatically erase the parts of the survivor's browser history that shows that the survivor searched for online help resources for domestic violence. The authors suggest that the app could be "hidden behind an innocent front end, such as a game app or an image gallery app." According to the authors, this design will prevent the perpetrator from recognizing that the app erases the survivor's history. A similar design could also be useful for an O-TPRS; however, such a solution will be ineffective if the perpetrator knows the pseudonym of the app. For instance, in their work on how technology aids perpetrators in stalking intimate partner violence victims, Freed et al. [111] outline many ways in which perpetrators can gain access to survivors' phones. Some ways include forcefully compelling survivors to unlock their phones, or strictly monitoring their activities. If a sexual assault survivor lives in an unconducive situation, (for instance, Section 4.4.1 and P22-SWSR in Section 4.4.1), having an O-TPRS app on their phones, even in disguise, may bring harm to the survivor.

Survivors could also forget to close the O-TPRS, or the perpetrator might see

them filling out the O-TPR form. The O-TPRS should be able to provide ways by which a survivor's privacy is protected if they leave their phone or computer unattended while filling out the form (see Section 4.4.1). The O-TPRS would also need to provide a way of easy escape on the app or the website if the perpetrator walks in on the survivor while they are filling the O-TPR form. Some sensitive websites have an escape button provided. These buttons allow people to exit the site quickly if they feel uncomfortable while reading the website's content or if it becomes unsafe to continue reading (for instance see [2]). Such designs could be looked into for O-TPRS apps and websites. Research needs to be done to determine how best such escape buttons could be placed on an O-TPRS and if they will be as effective.

It could be problematic for survivors if perpetrators know that an O-TPRS app was downloaded or the website was visited. By default, computers and phones save the history that an app was downloaded, or a website was accessed. This default setting is a challenge for survivors (see Section 4.4.1). If the perpetrator see this information, it could cause re-victimization of the survivor. For survivors of domestic violence, Arief et al. [11] suggest an app that automatically erases the survivor's web history. However, in abusive situations where the perpetrators check the survivors' web and installation history, we believe such a design could lead to more problems for the survivor. This problem could arise because the perpetrator may suspect that the survivors are trying to hide their activities by erasing their history.

Some technological solutions help people to surf the internet anonymously. For instance, to browse the web anonymously, people could use the incognito mode of their browser [58], or they could also make use of a Tor browser [35]. An option to hide survivors' online history could be for survivors to access the O-TPRS only in incognito mode or through a Tor browser. However, these designs require a certain level of familiarity with technology, and survivors may not find such designs usable (see Section 4.4.1). Further, incognito mode won't help in a scenario when the perpetrator has installed a key logger or is eavesdropping the traffic between the survivor's computer and the internet [1]. In addition, the Tor network is linked with so many illegal activities such as human trafficking and illegal sex trade [167], and as cited by P18-SWSR in Section 4.4.1, it may be hard for survivors to trust that

such systems can help reduce sexual assault.

Another option could be the inclusion of a process to verify a survivor's identity on an O-TPRS. This verification process could be done through an authentication system. Depending on the name supplied to the O-TPRS system, this design may not provide privacy because the presence of the app or website on a person's device may reveal to others that the person is a survivor. An authentication system may not fully protect the survivor's anonymity because whatever option is used to verify the survivor's identity could be an identifying factor of the survivor. This identifying factor could be the survivor's email address or biometric information. If a password system is used, this design may be problematic if survivors forget their passwords. If the survivor receives email to reset their login details, the perpetrators could see emails or email notifications, which compromises the survivor's privacy and anonymity. Further, if an authentication system is used, the O-TPRS would have to ensure that the police cannot access such identifying information without the survivors' consent.

After survivors send the O-TPR form to the police

After the O-TPR form has been sent to the police, the survivor's anonymity and privacy still need to be protected (see Section 4.4.1). Further, unauthorized individuals should be unable to discover that the survivor sent the information to the police (for instance, see Section 4.4.1). Protecting survivors' anonymity can be achieved by having security in place. Such a system will need high level of security, which is hard to afford especially for small organizations looking into developing O-TPRSs [114]. It is also difficult to measure how much security is good enough to protect a system. As argued by Hurlburt [162], security may never be good enough. The author explains further that for a secure system to be impenetrable by anyone, the system probably cannot be connected to the internet, and humans will have to be taken out of the loop [162]. The O-TPRS will hold very sensitive information from survivors. Therefore, whatever security measures the system employs, such measures should have a low likelihood of being breached. Any compromise of the O-TPRS could lead to distrust of the system and, even worse, further victimization of survivors (see Section 4.4.1, 4.4.1). The O-TPRS

operator will also have to convince survivors that such measures are good enough to protect their information.

4.5.4 The police trusting O-TPRS reports

The police want to be able to verify that the person who sends an O-TPR form is a survivor (see Sections 4.4.1, 4.4.2). However, it is unclear how this requirement can be achieved without violating the survivor's anonymity. One of the purposes of using an O-TPRS is to keep survivors anonymous to the police (see Section 4.1 and Table 4.2). Verifying the survivor's identity would violate their anonymity. In the P-TPRS, the presence of a representative at the TPR center may provide some assurance that the person making a report is a survivor (see Section 4.1.1). The police may trust that the report is valid because they trust the representative [46, 207].

Several solutions exist that provide verification of system users. Examples of such solutions include the completely automated public Turing test to tell computers and humans apart (CAPTCHA) [338]. However, current solutions such as CAPTCHA don't solve this problem, as CAPTCHA is designed to check if the user of a system is a human or not. CAPTCHA cannot verify whether the user of O-TPRS is a survivor or someone making a false report.

The cost of making a false report is low with O-TPRS. As explained in Section 4.1, a person is identified as a serial offender if three different survivors report them as an offender. Both O-TPRS and P-TPRS carry a possibility of false reporting. Nevertheless, the cost to a person who wants to create multiple false claims with P-TPRS is much higher. Such a person would have to convince two other people to walk into a sexual assault center at various times and accuse the same person of assault. With O-TPRS, the cost of making such false reports is smaller. A person could simply download the O-TPRS app or use the website and get two others to do the same. Alternatively, a person could make a report two more times from different accounts, known in distributed systems as Sybil Attack [83].

O-TPRS could lead to an increase in false reporting. Although sexual assault is an underreported crime, reducing the current barriers to reporting might lead to an increase in reporting. In addition, as explained by P1-SW in Section 4.4.1, the

use of O-TPRSs might also lead to an increase in false reporting. This is a major challenge, as this problem might reduce the credibility of real reports made through O-TPRS. This challenge is similar to swatting attacks where swatters make false reports to the police about an ongoing crime [19]. Similarly, in an O-TPRS, the possibility of false reporting could reduce the credibility of real reports.

A solution used to mitigate a similar challenge in other systems is the use of a password-based authentication to identify users uniquely. As discussed earlier, this solution, however effective, could reduce the anonymity of O-TPRS users. Further, users could easily create multiple email addresses to make false reports. It is unclear what measures can be put in place to deter illegitimate users while maintaining ease of use for legitimate users to report their sexual assault. Future research could investigate how O-TPRSs can implement a form of verification or CAPTCHA system for survivors. This system should be able to verify that the person reporting is a survivor. In addition, the system should not introduce the additional bottleneck of having human verification or reducing survivors' anonymity.

However, it should be noted that the motivation for making multiple or false reports seems weak. Although any report made will be registered in a database, and three reports would trigger follow-up from the police, as explained in Section 4.1, that follow-up would simply be an invitation to make a formal report, which the survivor was free to do at any time anyway.

4.5.5 The provision of human support

The importance of human support when reporting a sexual assault was discussed by many participants (see Sections 4.4.2 and 4.4.2). Participants explained that when using an O-TPRS, it would be important for survivors to have humans in the process for two reasons: 1. To ensure that the survivor receives the support needed to complete and submit the form to the police. Many participants wanted human support when filling out an O-TPR. It is unclear if this finding is primarily because most of our participants were already receiving support from sexual assault centers and therefore could not imagine using an O-TPRS without a support worker. It may be important to carry out further research to investigate if survivors who do not receive support from sexual assault centers will be comfortable using an O-

TPRS without human support. 2. To ensure that the survivor is in the right mental state to make a report of a sexual assault [291]. For instance, sometimes survivors deal with flashbacks or disassociation from the present moment and need support before, during, and after making a report [291].

To provide support for survivors, an option could be to provide human support via a video or audio call on the O-TPRS. While some participants thought this option would be useful, others suggested they would need face-to-face interaction (see Section 4.4.2). This design also doesn't address the problem of verifying that the survivor is ready to make a report [291]. It would be difficult for a human to verify over a video or audio call that a survivor was in the right mental state to make a report. This verification is important because on the O-TPRS, the survivor could write about their feelings rather than limiting the input to the factual details about the assault, and these details might be used against the survivor in the court of law (see Section 4.4.1). Further research is necessary to identify unique solutions to ensure that the survivor is ready, before submitting a report to the O-TPRS.

4.5.6 Balancing unlimited and limited input

There should be a balance between providing the survivor with too little or too much time and document space to complete a report. Too much time and document space in the O-TPRS could result in a survivor providing details that could be used against them (see Section 4.4.1). Implementing a document space limit on the O-TPRS may be helpful, however more research needs to be done to identify how much space is too much or too little and how such restraints may affect survivors' willingness to use the O-TPRS. Further, implementing a time limit could defeat the purpose of letting survivors complete an O-TPR form at their own convenience.

4.6 Conclusion

Our paper presents privacy and security challenges in designing an O-TPRS. It introduces many questions that need to be answered in order for survivors and police to trust and use an O-TPRS. Our research serves as a starting point towards designing O-TPRSs to increase sexual assault reporting and the arrest of perpetrators. We presented our findings to Vesta, and the organization is taking this report into con-

sideration in the development of their O-TPRS. We hope these results can start a discourse in the research community and lead to solutions for designing effective online reporting systems for sexual assault survivors.

Chapter 5

Initial Discussion: Tying it All Together

5.1 Generalizability of qualitative studies.

Generalizability is the "degree to which the findings can be generalized from the study sample to the entire population." [253]

Although qualitative studies are not generalized in the traditional sense or meaning of the term, population diversity and sample size may be more important based on the research questions [5, 65, 223]. When the research questions are focused on understanding the how, why, and getting in-depth knowledge of a particular phenomenon, having a diverse sample, which may not be generalizable in the traditional sense, has been recommended as more important in these types of studies. Because my dissertation is more exploratory and answering the how and why, I used a qualitative approach.

5.2 General Discussion

Based on our results in the previous chapters, the security and privacy challenges can primarily be categorized into two: technological challenges, which refer to challenges related to the design of the technology, and human challenges, which are the challenges that are specific to the user groups making use of the technological

solutions (see Chapters 2, 3, 4, 5). Table 5.1 shows the challenges that are grouped under human and technological challenges.

Table 5.1: The categorization of challenges into technological and human challenges

Categories of challenges	Chapter 2	Chapter 3	Chapter 4
Technological challenges	Technological dimension	a. The inability to delete a joint account and its content b. The frustration of losing personal content c. The risk of an account being hijacked by a secondary user	Technological concerns
Human challenges	a. Human dimensions b. Organizational dimensions c. Environmental dimensions	a. Cognitive burdens b. The uncertainty of whether the sharing was successfully stopped c. The annoyance of being unable to migrate content to anew account d. The burden of avoiding awkward conversations e. The stress of ending the sharing of utility accounts when the primary user moves out	Emotional concerns

We discuss the implications of the findings from our research. A major theme was that participants did not trust technology and therefore had various security and privacy concerns. Participants had multiple reasons for the distrust in technology, which we discuss below. Another overarching theme was power imbalance. In relationships and technology use, there was mainly the issue of a person having the upper hand in using technology. Participants feared that the person with the greater power could abuse/misuse the technology. For the rest of this chapter, we discuss the reasons for the distrust in technology, the issue of power imbalance, and the implication of our findings.

5.3 The dual use of technology

Our research highlighted the ease at which people use technological solutions for purposes other than intended. For instance, in using technological solutions to submit sexual assault reports, police officers feared that people could easily use the solutions to make false reports, leading to an increase in false reporting and a

distrust of legitimate reports (§4.4.1). The police officers were more comfortable with having a human in the reporting loop (§4.4.2). The police wanted a support worker to have interacted with the person making the report. On the other hand, because technology is used to promote rape culture and aid perpetrators, survivors found it difficult to believe that technology can also be used to report sexual assault (§4.4.1).

Further, in ending the sharing of online accounts, participants were concerned that account access given to a person when the relationship was going well could easily be misused when the relationship ends (§2.3). Similarly, in telecommuting, a participant gave her students remote access to her computer to facilitate learning. However, the participant was worried that the student could easily misuse the remote control that they have been given to access other parts of her computer (§3.5.2). In addition, some telecommuting solutions could aid with monitoring employees' or co-workers' activities and daily routine even during weekends (§3.5.2). All of these were security and privacy concerns raised by participants and led to the distrust of technological solutions.

Because of how easily technology can be misused, some participants would rather *not use* technological solutions even though these solutions could offer many benefits, such as increasing the reporting of sexual assault and reducing sexual assault incidents. The issue of the dual use of technology can also be seen in other technological solutions and lead to low adoption of those solutions. For instance, while smart speakers provide several benefits, potential users are worried that the speakers can easily be used to monitor and track their everyday activities, and hence there is low adoption of the devices [59, 281]. A similar situation is observed in the low adoption of other important technological solutions such as the COVID-19 contact tracing apps. While the apps could reduce the spread of COVID-19, there is low adoption because the apps could be used in a manner that wasn't intended which is a privacy and security issue for potential users [51, 184, 299].

There is a need for solution providers to design technological solutions to reduce the possibility of misuse. Some principles of designing secured systems could be used as a guideline to help solution providers build better technologies that could reduce misuse. For instance, the principle of safe defaults states that systems should be designed to be "fail-safe, meaning that they fail 'closed' (denying access)

rather than 'open"' [331]. This principle implies that the default setting for any secured product should be the *safe* option. Furthermore, in designing technologies, solution providers could think of various ways by which those technologies can be misused and try to accommodate for those. Kadri and Uusitalo et al. propose this approach to designing everyday technologies and termed the approach 'empathy by design' [170] or 'safety by design' [328]. Such a technological design may be unable to accommodate every abuse use case; however, it will go a long way in providing safer technological devices and platforms than those that currently exist and could increase the adoption of those solutions.

5.4 Lack of control when using technological solutions

Participants believed they had no control over the outcomes of using technological solutions and, therefore, found the solutions challenging to use. Therefore, participants wanted to use non-technological solutions instead. For instance, for the paper reporting version used in reporting sexual assault incidents, the survivor meets with a representative, either a nurse or a social worker, at a reporting center. The survivor fills out the form at the center and returns it to the representative before leaving the center (see §4.1.1). Participants believed they had more control over the paper version of reporting than using a technological system. Because of their link with the perpetrators, they were afraid of their perpetrators getting access to the reports. Participants believed that after they click the submit button on a technological solution and no longer 'see' the information, they have no control over what happens to the information afterward. However, this belief is ironic because participants also have no control over what happens when using the paper version of the reporting system. In many cases, after the survivor leaves the reporting center, the nurse or support worker fills out the survivor's report in an online system and sends it to the police. One reason participants believe they have limited control in using technological solutions is that whatever is kept online is available for everyone (see §4.1.1). Further, participants trust the support worker that they can see in person rather than an unseen entity they have no control over.

Furthermore, participants did not have a sense of control over what happened after they stopped sharing online accounts. For instance, participants had difficulty

remembering all the accounts they shared with the secondary users (§2.3). Furthermore, many online accounts require participants to have complex passwords which they cannot remember. Since participants believed they had no control over the type of passwords they are allowed to use, participants decided to use the same 'complex' passwords on multiple accounts. The reuse of similar passwords in multiple accounts becomes complex in ending account sharing as participants had to remember *all* their personal accounts and change the passwords to those accounts. In other cases, the primary users did not have a sense of control over the account as they faced a "racing problem" when ending password-based sharing. When account sharing ends, whoever resets the account password first wins the race by taking control of the account (§2.3).

In developing technological solutions, technologists could look into strategies for giving users a sense of complete control or ownership of the solution. In some cases, this challenge stems from participants not having a full understanding of how the technology solution works (§4.4.1). We suggest educating end-users about the solutions. For instance, such education could be done through automated onboarding when users start using the solution [250]. This type of education may help influence people's mental model about the amount of control they have in using a solution.

5.5 Protection of anonymity and privacy

In Chapter 4 we define anonymity and privacy. Privacy and anonymity are related but can be differentiated in some contexts. Webb [340] defines online privacy as the ability to "control who (if anyone) sees what activities you engage in online. In other words, 'they' can see who you are, but not what information or websites you access or seek." The author further defines anonymity as, "when you opt to have your online actions seen, but keep your identity hidden. [This means that] 'they' can see what you do, but not who you are." In other words, privacy means knowing a person's *identity* but *not* their *actions* in the system. Anonymity means knowing the *actions* of a user in the O-TPRS system but *not* the user's *identity*. Table 5.2 below (from Chapter 4) illustrates these definitions.

We discovered that in all technological solutions regardless of the context par-

	Know my actions	**Do not know my actions**
Know my identity	No privacy and no anonymity	Privacy but no anonymity
Do not know my identity	Anonymity but no privacy	Privacy and anonymity

Table 5.2: Privacy and anonymity illustrated.

ticipants wanted either their anonymity, privacy, or both protected. But in some cases, this wasn't possible and therefore was a concern for users.

For instance, in reporting sexual assault, the *action* for the survivor is: filling a sexual assault report. And their *identity* in this context is: victims of sexual assault. The survivors wanted this *action* to be known to the police (but not unauthorized people) but wanted their *identity* (privacy) protected. However, the police wanted to know the *action* and the survivor's *identity* (i.e., no privacy or anonymity for the survivor). As seen in Chapter 4, this was a clash of priorities for both stakeholders (the police and the survivor). The challenge for the sexual assault reporting technology designers is that without finding a solution that can satisfy these two stakeholders, it is unlikely that either will trust such solutions.

In telecommuting, the *action* for telecommuters is: to do their organization's work. Their *identity* in this context is: workers. Telecommuters wanted controlled privacy. They did not wish for any other form of their identity to be compromised. Telecommuters only wanted to be known as a 'worker' to their co-workers. They did not necessarily want to be known as a mum, a dog owner, a husband, or an artist. But this was not possible as, during telecommuting, workers had to engage in video calls and *invite* people digitally into their homes (§3.5.2). Further, there was the fear of co-workers being able to monitor employees' daily routine through telecommuting solutions monitoring capabilities (§3.5.2). In using telecommuting solutions, telecommuters wanted control over their privacy and what aspect of their lives they decided to show to their co-workers, which was not always possible.

In ending a shared account, participants wanted a situation whereby when they stop sharing an online account, their previous *actions* while using the shared accounts are protected (anonymity) as well as their *identity* that may have been shared while they performed those actions (privacy). However, participants' privacy and anonymity were not always provided, which led to various user-centered chal-

lenges (Chapter 3).

In designing technological solutions, technologists should consider the anonymity and privacy that people need and ways of providing it to them. Solution providers need to rethink people's various identities and actions and consider to what extent people want their identities and actions protected. Solutions need to consider people's privacy boundaries and how technologies invade the privacy boundaries that they have set in their everyday activities [6, 241, 323]. This consideration could lead to providing solutions that people will be more comfortable using.

5.6 Solutions do not implement the principle of least privilege

Participants were hesitant to use technological solutions because a compromise of one solution could compromise many other solutions. This finding is a violation of an important security principle known as the principle of least privilege. van Oorschot [331] define this privilege as the need to "allocate the fewest privileges needed for a task, and for the shortest duration necessary." Adhering to this principle may help improve the security and privacy of users of technological solutions. For instance, in ending shared accounts, participants were worried because sharing their password for one account meant that the secondary user also knew the password for many other accounts since participants reused passwords. Therefore, if the participant forgets to change the similar passwords used in other accounts, that gives the secondary user unrestricted access to other accounts (§2.3). A suggestion could be for technologists to design solutions that do not allow the reuse of passwords across systems. The solution could scan the person's computer and prevent the person from using a password that has been previously used. While this suggestion may help avoid the reuse of similar passwords, it adds the complexity of users remembering the complex passwords used across various accounts. A better solution would be for authentication systems to be designed without the use of complex passwords. For instance, in their paper [28], the authors discuss the replacement of passwords with more usable user authentication methods.

Further, participants in the study on sexual assault reporting were concerned about using an app on their phone (compared to a website) to report sexual assault.

This concern is because a compromise of their phone security also compromises the sexual assault reporting app (§4.4.1). Most authentication systems provide all but nothing type of authentication. Therefore, once an attacker can compromise the security of a person's phone, the attacker can interact with all the apps on the phone. Both previous and current research shows how technological solutions, especially mobile, can offer more fine-grained user permissions [347, 348]. We suggest technologists look into implementing these solutions.

5.7 The challenges of using technological solutions could lead to life threatening situations

In designing technological solutions, technologists need to note that while users experience most of the challenges online, these challenges could have offline consequences. For instance, in telecommuting, users were worried about of people locating their homes and attacking them and other household members (§3.5.3). In ending shared accounts, there was the risk of account hijacking and impersonation (§2.3). Furthermore, survivors of sexual assault were worried about a technological solution malfunctioning, and perpetrators discovering that the survivor had used or attempted to use a solution to report sexual assault. This problem could lead to re-victimization of the survivor (§4.4.1). Addressing the challenges involved in using these solutions becomes even more critical for the safety of users.

5.8 Power imbalance

An overarching theme in our findings is power imbalance in using technology in relationships. We define power imbalance as "the ability of human agency to exercise control over its social and physical environment" [119]. The author further explains: "Power imbalances exist in a social setting, when there are asymmetrical relations of power among persons. ... A power imbalance exists when A has more control or influence over B's behaviour than vice versa. Control may be exercised by the use of superior force, or by economic means, or by control over knowledge and information" [119].

Technology use in relationships currently puts one user above the other through the design of technology. This situation sometimes leads to unfair privileges to the

user with the lesser power, especially when the relationship breaks down. The power imbalance can lead to the abuse of technology by the user with the greater power. For instance, in a shared account, when the account sharing ends, the primary and secondary users face a *racing condition*. The first user that can successfully change the password gain full control of the account and can misuse the account as desired (for example, a user can hijack the account, see Chapter 2). In telecommuting, the power imbalance between the employer and the employee forces the employee to use technology in ways they do not prefer (for instance, giving remote control of teleconferencing technologies to clients, turning on their video cameras during meetings, or having online monitoring indicators on). Participants were fearful that these privileges could be abused, see Chapter 3.

The power imbalance is also a reason for participants' distrust of technology. For instance, as discussed, users felt a lack of control when using technology. It always seems like the user with a 'better understanding of technologies' had the most say on using technologies in relationships.

A balance in power dynamics will go a long way in addressing people's security and privacy challenges in using technology in relationships. To reduce the abuse of technology, we need to understand the inherent characteristics that make it easier for technology to be manipulated by the user with greater power. An understanding of these characteristics could help to reduce the power dynamics and potential abuse of technology.

In the following Chapters, we uncover these characteristics and discuss the implications of our findings for designing and developing technological solutions for relationships.

Chapter 6

The Characteristics of Technology that Facilitate Misuse

Using the complex relationship scenario, we conducted research to understand the inherent characteristics of technology that facilitate abuse.

Our research question was:

- RQ5: What characteristic of technology facilitates abuse?

Answering this research question will help us in identifying the attributes of technology that facilitate abuse.

We addressed our research question by conducting a literature review of 224 research papers—the papers discussed how technology facilitates the sexual assault of victims by perpetrators. We analyzed the papers using grounded theory.

For clarity we define the following terms.

Technology: A collection of systems "that allow users to exchange digital information over networks" [32]. In this paper, we use technology as an umbrella term for all types of mobile, web-based, and internet-enabled services, platforms, and devices.

Sexual assault: "Unlawful sexual activity and sexual intercourse carried out forcibly or under threat of injury against a person's will or with a person who is beneath a certain age or incapable of valid consent" [341]. For the purpose of our study, we treated sexual abuse and rape as particular types of sexual assault. We

also refer to sexual assault as "assault" when the context is clear.

Perpetrator: "A person who carries out a harmful, illegal, or immoral act" [181]. In the paper, we refer to the perpetrator in the context of sexual assault.

Victim: A person who has been sexually assaulted.

Target: Person(s) the perpetrator aims to assault sexually.

Stakeholders: Actors (persons or organizations) with a vested interest in a certain course. We use stakeholders to refer to volunteers and staff of sexual assault centers, police officers, and people working to provide legal services to victims.

Re-victimization: Refers to victims reliving the sexual assault experience, either physically or psychologically.

Our specific contributions are:

- We performed the first systematization of knowledge on the characteristics of technology that facilitates abuse.
- Second, we identified ten characteristics of technology that facilitate sexual abuse. These characteristics are covertness, anonymity, evolution, boundlessness, reproducibility, accessibility, publicness, indispensability, malleability, and opaqueness.

6.1 Method

We used a five-step iterative process combined with coding from Grounded Theory to review the literature, for the systematization of knowledge. We chose this approach because it allowed us to reach a "thorough and theoretical analysis of any topic" and provide insights grounded in the literature [350]. We followed the five-step iterative process itemized by Wolfswinkel et al. [350]: Define, Search, Select, Analyze, and Present. Two of the authors selected 224 papers (we discuss the paper selection process below). All authors then conducted a card sorting exercise and several brainstorming sessions to arrive at our findings. For the rest of this section, we explain the five-step process that we used for our systematization of knowledge. It should be noted that we iterated between the steps as needed, as the process is meant to be iterative [350].

Defining: The goal of this step is to define the scope of the literature review. During this step, we defined our:

Inclusion criteria- For a paper to be included, it should satisfy all of the following criteria: (a) it must be a peer-reviewed journal article, conference/workshop paper, or book chapter, and (b) it must discuss sexual assault, and (c) it must discuss the use of technology to facilitate, report, or prevent sexual assault.

Exclusion criteria- We excluded papers that discussed sexual harassment (i.e. making rude, sexually degrading, or offensive remarks or gestures) but not sexual assault.

Selected source/database- We chose Google Scholar (scholar.google.com) to search for the papers used in this research because it provides a broad coverage of research topics [136, 227, 243, 316].

Specific search terms- We searched using either 'technology' or 'social media' term combinations with each of the following terms: sexual assault, intimate partner violence, IPV, human trafficking, abuse. For example: (i) technology human trafficking, (ii) social media sexual assault.

Searching: The goal of this step was to search for papers using the search terms defined above. We searched using Google Scholar. While searching, we realized from the title(s) and abstract(s) of the resulting papers that we may miss out on other relevant papers if we used only the search terms defined initially. Therefore, we went back to the previous step and added the following search terms: social networks, child abuse, domestic violence, intimate partner abuse, technology-facilitated abuse, sexual crime, sexual violence, COVID-19 sexual abuse, perpetrators, sexual abusers, rape, rapists, smart devices sexual abuse. Two researchers conducted this step independently. 258 papers were identified at this step.

Selecting: The aim of this step was to check if the papers identified in the Search step (i.e. papers identified by using the search terms) satisfied the inclusion criteria specified in the Defining step. For each of the papers identified during the Search step, we did the following: (a) Checked forward and backward citations to see if any of the papers that were cited or did cite a given paper also met our criteria. Through this process, we added 154 new papers, resulting in a total of 412 papers. (b) Proceeded to filter out duplicates (e.g., almost exactly the same papers, one version published in a workshop and the other at a conference). After purging duplicates, we were left with 321 unique papers. (c) Read the full text of each paper in our data set to determine if it met the inclusion and exclusion

criteria. As a result, 91 papers were removed, leaving us with 230 papers. (d) Of the 230 papers, six papers were from 1994-2004. After reading them, we decided to remove them because the type of technological tools described in the papers were so outdated that they were no longer relevant (for instance [104]). We ended up with 224 papers that we could use in this research; they were all published during the period from 2005 to January 2021. Two co-authors were involved in the first three steps. All authors were involved in the last step.

Analyzing: The aim of this step was to analyze the papers in the selected sample. We analyzed our data in ascending order of publication date, in order to see if specific trends emerged over time. As suggested by [350], we employed coding techniques from Grounded Theory as follows: (a) Open coding: We read papers and highlighted those parts of each paper that appeared relevant to our research questions. We then assigned one or more codes to each highlighted text fragment. One of the co-authors performed open coding for each of the papers in the dataset, and another coded 150 papers of the dataset that were published most recently. Two researchers met frequently online to discuss their interpretations of the codes, and to resolve any disagreements. As a result, a total of 148 individual codes were generated. (b) Axial coding: Each of the two co-authors independently grouped codes identified during open coding into a set of categories and then they met online to discuss the differences and to converge on a single set of those categories. Instead of quantitatively measuring the agreement between the two researchers, we focused on using the differences to have a discussion about the best way to interpret the codes [324]. As a result, the researchers arrived at a set of nineteen categories. (c) Selective coding: All co-authors discussed labels and semantics for all of the categories, and arrived at a consensus. We resolved our differences by inquiring about the reason(s) behind the category label(s), and discussing the idea(s) that surrounded the labeling of the category, while trying to reach a consensus that all co-authors agreed with. Afterward, we performed a card sorting exercise to determine the relationships between the categories. We also had several brainstorming exercises to better organize our findings. As part of those exercises, we selected main and sub-categories, which are presented below. We reached saturation in this process when no new revisions emerged.

Presenting: All co-authors organized the key insights that we derived from

the categories and the relationship(s) between them. We present our findings in the following sections.

6.2 Results

6.2.1 How Technology Enables Abuse

We present the characteristics of technology that facilitate the abuse of victims.

Covertness

We define the covertness trait of technology as the characteristic that enables one to operate technology in a particular location without the knowledge of the impacted individuals. This trait allows for perpetrators to subtly gather information about or monitor targets and victims. This characteristic can mostly be seen in mobile or IoT devices [192] and spyware [202, 307]. Abusers could also hack into other non-IoT devices, the victims' email, social networking, and media accounts (such as Facebook, dating sites) and covertly use or gather information [97, 137]. We discuss below some of the technological tools used covertly by perpetrators and how these tools enable abuse.

Perpetrators use technological tools that enable surveillance of another person but not vice versa. Chatterjee et al. define these types of technological tools as subordinate tracking devices, and they enable a person to monitor another but not vice versa [52]. Perpetrators could misuse these tools to gather information about victims covertly [52, 135]. For instance, Westmarland et al. describe 'track your wife', a mobile app that runs in the background of a device where it is installed. The app periodically sends time and the device's geolocation to a server. Using this information, a perpetrator can know the device location (and in other words, the location of the victim) [342]. Another example is the use of auto-answer phones. These are phones that have the ringer on silence and automatically answer calls. Perpetrators could leave these phones in the victims' cars, houses, or other locations and call the phone to listen in on the victim's conversations without their knowledge. Using the information gathered from the victims' conversations, the perpetrators can determine the recent activities of the victim and plan a suit-

able time and place to abuse the victim [200, 308]. Perpetrators could also use parental apps and 'track my pet' apps to monitor victims [84]. Further, perpetrators could use spyware [29, 86, 146, 202, 221, 222, 307], screen, audio-visual and voice-activated recorders [322].

Perpetrators use personal and mutual tracking technologies. Chatterjee et al. define personal tracking apps as those that are "intended for use solely by the owner of a phone" (e.g., find my phone apps) and mutual tracking as "apps that allow a group of people to track each other's locations" (e.g., apps to track family members) [52]. For example, the location of victims who are fleeing from perpetrators to various shelters could be revealed by the GPS technology of their mobile devices [118]. Many studies report various means by which perpetrators misuse both personal and mutual tracking apps to monitor victims discreetly [12, 45, 52, 69, 81, 84, 87–89, 110, 123, 129, 131, 132, 185, 187, 195, 200, 202, 210, 222, 273, 276, 288, 311, 314, 330]. Perpetrators can also surreptitiously use other technologies for surveillance, such as IoT devices [27, 54, 186, 245, 280, 315, 356], hidden cameras [84, 107, 108, 110, 117, 135, 138, 146, 200, 256, 266, 276, 311, 322, 342, 352] and many other types of technological tools [12, 29, 45, 52, 81, 84, 87, 89, 131, 133, 138, 187, 195, 210, 273, 288, 311].

Tracking functionalities are available by default on some technological devices, which provide more avenues for victim surveillance. Some of the tracking functionalities are provided with the device's operating system or by the device service provider, which means users are unable to uninstall these apps: Chatterjee et al. describe some of these instances, *"Verizon Family Locator do not require an abuser to install an app on the phone [to monitor victims], and often can be remotely activated with the credentials attached to the account that pays the cellular bill. Android natively provides tracking functionality, via Find My Device, or via Google Maps' unlimited location sharing functionality. Assuming the abuser has access to the victim's Google credentials, the abuser can remotely turn on the Google Maps Timeline feature and obtain periodic (even historical) information about the victim's location."* [52].

Apart from surveillance, perpetrators subtly compromise the victim's online accounts to impersonate them or use their information. Researchers report incidents where abusers have garnered information about victims from their com-

promised accounts without the knowledge of the victim [107, 256]. Fraser et al., for instance, described the case of a police officer who wanted revenge against his girlfriend and gained control of her email account. The officer used the email account to impersonate her on a dating site and arranged for seventy men to meet up at her home [107].

Perpetrators appear to be omniscient and omnipresent, creating more avenues for the abuse to continue. The covert trait creates a *Big Brother* effect whereby the perpetrator always has up-to-date information about the victim and could have an upper hand over them. Because of how discreetly technology is used, victims may not know the abuser's activities [76, 107, 137, 256, 257, 342, 352]. The omnipresence and omniscience effect makes it hard for victims to distance themselves from perpetrators, which leads to more opportunities for abuse [107, 352].

Perpetrators coerce victims to indulge in sexual acts because of the sensitive information perpetrators have about them. The perpetrator could gather a significant amount of information about the victim, including sensitive surveillance videos, images, or audio recordings. To sexually assault victims, the perpetrator could blackmail and threaten to share the sensitive information obtained from covertly monitoring the victims [85, 146, 185, 254, 290, 311, 352]. Because of the fear that the perpetrator will fulfill the threat, victims keep engaging in sexual acts with the perpetrator [336].

Publicness

In most cases, information kept on the internet is public. Unlike the covertness characteristic that deals with collecting non-public information about victims, the public characteristic refer to publicly available information created when a person uses technology.

Perpetrators use social media sites to gather information about targets or victims. A lot of personal information is displayed on social networking sites and other social media apps. These social platforms include Facebook, Instagram, Twitter, Linkedln, etc. Through these online networking platforms, perpetrators can learn about their target's likes, dislikes, interests, geo-location, school or work

information, and other personal information. Perpetrators can then use the information to build an online relationship with the target and proceed to offline meetups to sexually assault their target [26, 29, 77, 84, 107, 176, 200, 202, 215, 311, 352]. Perpetrators can also learn current information about their past victims to facilitate the continuation of sexual abuse [77, 88, 176, 352].

Victims find it challenging to avoid perpetrators monitoring them using their publicly available information. Many research papers report this challenge [118, 202, 352]. Sometimes, the perpetrators are still friends or connected with the victims' friends or others in their networks on social media and other online platforms. Therefore, the perpetrator can use these platforms to get current information about the victims (such as the victim's location and activities) through their friends on social media. The perpetrator could use this information to locate the victim and continue the sexual assault [185, 352]. Further, victims living in shelters had difficulties hiding their exact locations from perpetrators because of publicly available social media information. Matthews et al. explain the issue: *"An important challenge in staying hidden was that the abuser could use other people—such as the survivor's children, family, friends, colleagues, teachers, and so on—to find their contact or location information [online]. This concern ... greatly complicated the survivors' online privacy and security work, because it required them to enlist the cooperation of other people who may not fully understand their situation."* The paper further reports that in an attempt to stop the perpetrator from using their publicly available information, victims sometimes had to restrict their children's social media activities or to block mutual friends that the victims have with the perpetrators [202].

The default settings of websites make information publicly available. Using some online platforms could lead to the disclosure of some information that people do not want to make public [107, 129, 185, 202, 311]. For instance, Facebook allows people to tag other users in posts or photos by default [94]. This setup could help abusers know their targets' locations or determine recent activities they have engaged in. Users would have to manually change these settings.

Some apps facilitate the aggregation of various publicly available online data. Such aggregation could be useful to perpetrators. Dimond et al., for instance, discussed an app, Google buzz, that collated people's online identities from

various websites. The authors explained the challenges, "When Buzz launched, it disclosed all the names of Gmail contacts publically. For one blogger, this was extremely problematic because the service automatically shared her comments on Google Reader with her abusive ex-husband, which resulted in the disclosure of the locations of her home and work." [77]. Perpetrators have exploited similar apps to assault victims or targets [146].

Anonymity

We define anonymity as the ability to hide one's true identity when using technological tools. Anonymity is provided in various forms of technologies, especially in using the internet or mobile cellular devices.

Perpetrators create false identities that facilitate in-person meetings with targets. Using some technologies such as the internet helps people hide under many anonymity layers [116, 176, 268, 274, 336]. For instance, Tor internet web browser facilitates the protection of people's identity online by providing a secured network for communication [263]. Because of the anonymity that technology provides, perpetrators could create a false online persona that people would most likely find appealing and be willing to engage with [26, 67, 176]. Multiple papers report incidences where the internet facilitated anonymous grooming of potential targets and the eventual in-person meeting between the perpetrator and the targets [92, 214, 336]. Further, perpetrators can create multiple false identities by creating many online accounts and profiles on various websites [26, 85, 92, 204, 214].

Perpetrators build social trust between themselves and the targets. The anonymous friend feature of several social networking sites (SNS) helps victims in trusting a perpetrator. Online social media is built on the network and concept of friendships [358]. Being friends with strangers on some social media platforms could make people assume they know a stranger when, in reality, they do not [268]. Kloess et al. note that the constant anonymous communication on the internet helps to *"foster feelings of belonging and a sense of community to form relationships and building friendships." [176]*. These 'feelings' help create the notion that a stranger is a friend and leads targets to trust the perpetrator. For instance, research shows that victims of technology-facilitated abuse report an increased friendliness

or false sense of 'knowing' the perpetrator online before they met in person [26, 36, 268]. Similarly, the idea of social trust can be seen in online dating sites and apps. Perpetrators create a false online persona on dating sites and build trust with the targets. [60, 107, 256, 336]. Unfortunately, people could be more emotionally vulnerable with dating sites and could end up trusting an appealing stranger more easily [256, 293]. Further, research shows that perpetrators use a combination of technological platforms. For instance, while the initial point of the meeting could be a social media platform, however, the perpetrator continues the conversation on other technology platforms such as through mobile phone communications (e.g., text messages and calls) to build social trust [26, 36, 74, 157, 176, 204, 216].

Anonymity and a heightened sense of social trust leads to eventual in-person meetings. The anonymity of the technological tools leads to victims trusting the fake identities that perpetrators have developed online. Perpetrators exploit the false sense of connection and relationship provided by these sites to facilitate offline meetings and sexual assault of targets [26, 36, 204, 256, 274, 336]. The idea of confidence and social trust is similar to the literature of how con men gain their victims' trust through confidence games (also known as cons) [141, 143, 238, 317].

It is difficult to hold a perpetrator accountable. Because of the complex layers of anonymity (such as the encryption of online communications), law enforcement finds it hard to identify and apprehend perpetrators [213, 217, 247]. In addition, as explained above, perpetrators make use of multiple technological tools in contacting targets. These tools have varying anonymity levels and add to the difficulty of apprehending perpetrators [146, 247]. The knowledge that anonymity could make it challenging for law enforcement to apprehend perpetrators could develop more confidence in perpetrators and, therefore, a continuation of the crime of sexual abuse [10].

Evolution

New technologies are constantly being developed, and old technologies are being improved. Technology, therefore, is ever-changing and ever-evolving.

Advances in technology are creating avenues for alternative forms of abuse weapons. The evolution of technology can be seen in the development of many

new technological devices and online platforms [180]. While the evolution of technology is essential, it expands the perpetrator's repertoire [107, 159, 268, 269, 274]. Technological tools can also be used in ways that were never intended. Research shows that perpetrators weaponize technological evolution to scale up their offenses [30, 107, 204, 254, 276, 330, 342]. For instance, perpetrators make use of various online platforms to facilitate the distribution of unauthorized sexual recordings [147, 217], real-time instant messaging services increases the speed of communication between targets and perpetrators [159], the use of search engines, chatrooms, SNS, emails, online dating sites, mobile phones to locate targets [56, 92, 108, 116, 159, 176, 199, 204, 256, 293, 336], and the use of spyware and multiple IoT technologies to monitor targets and victims [26, 27, 84, 107, 192].

Further, even when a method of abuse is taken away from abusers, technological advances provide new and better ways to carry out abuse. Many research papers illustrate various ways by which perpetrators have adapted to use other means of technological abuse once a technological abuse tool is taken away from their toolbox [30, 204, 330].

Boundlessness

We define the boundlessness characteristic as the lack of geographical barriers. Technology is not confined to a particular space or geographical location. This characteristic is mostly seen in technologies that make use of the internet.

Meeting fellow perpetrators and forming a massive online community of support is easier. The internet's boundlessness characteristic makes it easier for perpetrators to form ties with many more perpetrators, share tips and strategies, and strengthen their network [157, 268]. Before the use of the internet, such a strong support network and collaboration among perpetrators would have been impossible [26, 157, 204, 256]. The characteristic allows for more like-minded people to come together on the various online platforms, with the goal of bonding, exchanging ideas about their sexual fantasies, identifying tools that could aid surveillance, and facilitating online and offline sexual meetups with targets or victims [67, 204]. Perpetrators use these communities to get others interested in being part of a sexual crime. Kloess et al. explain: *"In terms of offending behavior, such communities*

may also have changing effects on users' views due to its supportive and understanding, as well as justifying and normalizing, features." [176, 268].

Further, perpetrators can meet more targets. The characteristic opens up more opportunities for an abuser to meet more targets from various physical locations in the world [67, 91]. Technology gives *"expanded access to victims for offenders."* It provides the, *"ability by perpetrators to span large distances and involve multiple parties, to the extent that it outstrips the capabilities of many [police] agencies."* [213].

Perpetrators can continue the abuse of an ex-partner and blackmail them. The abuse can continue long after the relationship has ended. This problem stems from people sharing their online space while in a relationship. Even though their physical relationship has ended, ending their online relationship could be complex [311]. Hand et al. explain that because of technology, *"geographic and spatial boundaries no longer present a barrier for one to communicate, contact or locate another globally."* [129]. Technology is *"redefining the boundaries of romantic relationships in ways that provide a fertile ground for conflict and abuse and through providing opportunities for constant contact through mobile or online communication technology.* [86]. Sometimes, abusers still have access to victim's previously shared online accounts and can use the information on those accounts to blackmail the victim into engaging in sexual acts [110]. Technology therefore, *"lessens [the] personal sense of privacy boundaries."* [88].

Reproducibility

We define reproducibility as the ability to duplicate any information kept on the internet. This makes the information on the internet to be close to permanent.

Sexual content shared online is easily duplicated, resulting in re-victimization. Abusers sometimes share sexual images, videos, or audio recordings of victims on the internet. When this content is shared, it can easily be reproduced, making such information close to permanent [12, 80, 85, 92, 100, 139, 140, 144, 152, 153, 156, 206, 214, 217, 248, 254, 259, 261, 336]. Many research papers document the difficulties survivors face in attempting to remove content that has been reproduced on various online platforms [26, 80, 92, 254]. In situations of unauthorized du-

plication and distribution of sexual content and people engaging with the content, victims have described such incidents as feeling as the rape was occurring all over again [41, 67, 80, 255, 336].

Perpetrators can blackmail victims by threatening to post victim's sensitive information online. Perpetrators sometimes coerce victims' consent to engage in sexual activities and threaten to share sexual content online if they refuse or report to the police [26, 85, 151, 159, 274, 276]. Sometimes victims are afraid that the perpetrator will make good on their threat, and their sex images or videos will be visible online forever [256]. The victim, therefore, continues the sexual activities with the perpetrator [60, 101, 151, 152, 213, 260, 336].

Accessibility

Accessibility refers to technology being available and easily accessible to multiple individuals.

Perpetrators do not have to be tech-savvy to use technology for abuse. Technology is widely available, and because of how easily available technology is, perpetrators, do not have to be sophisticated technology users to abuse technology. Ramsay et al. explain, "the widespread uptake and everyday use of smartphones and connected devices in the home means that stalking and abuse online is no longer solely the domain of the most 'tech-savvy' perpetrator." [276]. The increased accessibility of technology is enabling perpetrators to easily monitor and abuse targets and victim [26].

Indispensability

We define indispensability as the characteristic of technology that makes it essential in everyday life. It is the attribute that leads to people being reliant on technology.

The constancy of technology in people's lives enables perpetrators to have access to victims consistently. The use of technological tools and platforms has become a necessary part of people's everyday lives [84]. The overall dependency on technology makes it harder for people to let go of technological tools while making it easier for perpetrators to get more targets [56, 176]. Some sexual abuse

shelters request victims to let go of technological use to prevent perpetrators from tracing them to their current locations or shelter facilities. However, victims find this request hard to adhere to [53]. People have become so dependent on technology that they find it challenging to cut off from technology even if it comes at the risk of sexual assault [26].

Malleability

We define malleability characteristic as the ease with which digital content can be tampered with. Many technologies can modify digital content, such as photoshopping a picture or altering a video and audio content using artificial intelligence. Perpetrators circulate modified sexual content of victims to facilitate revictimization [336].

Opaqueness

We define opaqueness as referring to a system with contents that are mysterious to the user. In our case, the system is technology.

Victims were concerned that they did not know the type and volume of data that their technological device has or collects about them. For instance, victims in a research study complained about how they knew that their IoT device was collecting data about them. Still, they could not figure out or remember what data collection they had consented to. Sometimes, victims had an incomplete mental model of these devices, and they either underestimated or overestimated what the device could do [27]. For the victims, the technological device is opaque [186, 314].

There is a cognitive workload for victims in remembering details about accounts that they use. This problem made it difficult for victims who wanted to cut ties with their abusers completely. Because technology is opaque, victims did not know or remember who had access to their online accounts. Victims were, therefore, still linked to the perpetrator after a relationship ends even though they wanted to cut all ties [187].

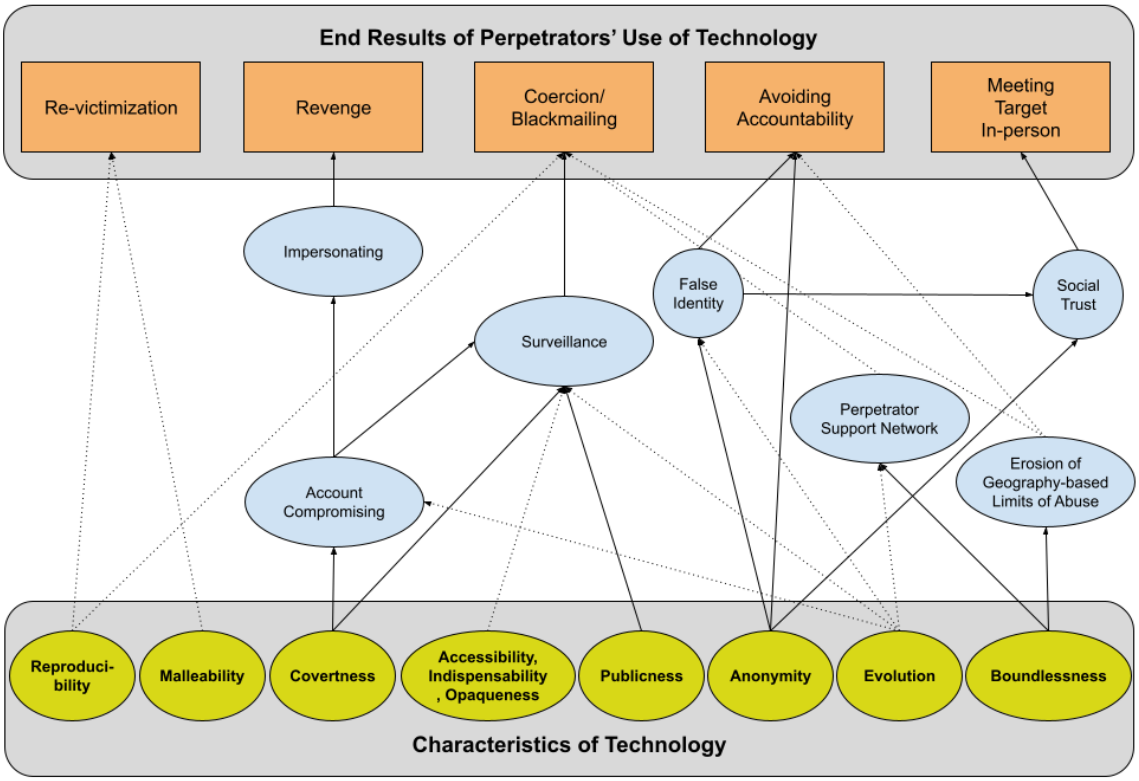

Figure 6.1: Visual summary of the results on how technology facilitates abuse. Solid/dotted lines indicate that specific characteristics enable/amplify perpetrators' capabilities. Note that false identity is when someone uses stolen or fabricated personal information. Impersonation is when someone pretends to be you [39]

.

6.3 Limitation

Our systematization of knowledge centered mainly on research work in developed countries. These may have influenced our categorization of technology's attributes. However, most of the research papers we found in the field of technology-facilitated abuse centered on developed countries. Further, we do not specifically focus on the link between technology and child sexual abuse. In addition we did not account for the differences between pseudonymity and anonymity.

"Anonymity can be defined simply as being without a name or with an unknown name. Pseudonymity is the use of a false name" [169]. However, the differences between these terms were not the goal of our research.

As with any qualitative research, our findings may have been affected by systematic biases [78]. To reduce researcher bias, multiple researchers were involved in analyzing the data and converged on their interpretations [227, 243]. Furthermore, we used only Google Scholar to search for papers, which might have introduced additional system bias. At the same time, Google Scholar's inclusive and unsupervised approach appears to provide the most broad coverage of papers [136, 227, 243, 316].

Despite of the above limitations, we believe that our study provides a useful background for future research on using technology to support victims and reduce sexual assault. Further, through our research, we identify characteristics that facilitate abuse in using technology in various types of relationships.

Chapter 7

Concluding Discussion: The Dimensions of Technology

We propose a design rubric to help developers and designers predict some security and privacy challenges users could encounter while using their solutions. Our findings in Chapter 6 show ten characteristics of technology that facilitate abuse. These technology characteristics are covertness, anonymity, evolution, boundlessness, publicness, reproducibility, accessibility, indispensability, malleability, and opaqueness. These characteristics facilitate abuse, which leads to security and privacy challenges. Therefore, considering these characteristics in technology design could help predict some security and privacy challenges users could face using the technology. This knowledge could lead to putting measures in place during the product development to help mitigate the predicted security and privacy challenges. Such measures could go a long way in preventing some of the identified risks of using technology in relationships. The characteristics discussed below were chosen based on the results from the individual chapters. Note that application of the characteristics as discussed in this Chapter have not been tested and further research is needed to test the application. In predicting some of the security and privacy challenges of using some technological solutions, we first need to define:

- The technology: This refers to the technological solution.
- The user: This is the person who will make use of the technology. For

example, with Facebook, this could be adults between the ages of 18-75 years old. Note that the user could be multiple personas.

- The action: This refers to the action that the user wants to carry. There could be multiple actions, but it's important to focus on one action at a time. For example, user actions on Facebook could be, make a public news post, tag users on a photo, share location, etc.

To apply the technology characteristics in this context, we need to look at characteristics as dimensions. For instance, with the Anonymity characteristic, the dimension can range from a system that provides *Anonymity* - to one that provides a *Controlled Form* of Anonymity. We are defining 'controlled form' as one where the user can determine when and if they want that characteristic of technology - to *No Anonymity*, which means that to protect the user's security and privacy, the user desires no anonymity in the system. We know these dimensions are not black and white, and since these are inherent characteristics of technology, it is therefore hard (if not impossible) to have, for instance, completely no anonymity. But having this knowledge could, to a large extent, help developers design systems that try to mitigate these challenges and, as much as possible, provide better user scenarios. For the rest of the Chapter, we use the design rubric, showing how technology characteristics facilitate some security and privacy challenges identified in previous Chapters. We chose these characteristics by looking at the results section of previous chapters and identifying the characteristics responsible for the identified security and privacy concerns. Please note that this list is not exhaustive; they are only examples. We also provide recommendations on how some challenges can be addressed. It should be noted, however, that proper evaluation of these countermeasures is subject to future research.

7.1 Technological Dimensions related to the Security and Privacy Challenges of Ending Online Account Sharing (Chapter 2)

Technology: *Online shared accounts.*

Users: *Primary users.* Note that for this discussion we chose primary users. An-

other user type could be the secondary user. For this type of user, there may be other security and privacy challenges and related technological dimensions.
Action: *Ending the sharing of online accounts.*

7.1.1 Opaqueness

(refers to a system with contents that are mysterious to the user. In our case, the system is shared accounts)

Figure 7.1: Figure showing the current and ideal technological dimensions for *Opaqueness* in shared accounts.

1. **Remembering secondary users (see Section 2.3)**. Primary users could not remember which secondary user was on an account because the technology was opaque. Participants wanted to easily figure out the people using the account at any point in time. In an ideal world, participants wanted a system that was not opaque.

2. **Changing passwords (see Section 2.3) and remembering which passwords are reused on which accounts (see Section 2.3)**. Changing passwords can be a tedious process when account sharing ends. Participants needed to remember which account used a similar password to change the password. However, participants had multiple accounts, and with the technology being opaque, participants found it hard to determine which accounts made use of passwords similar to their shared accounts.

3. **The uncertainty of whether the sharing was successfully stopped (see Section 2.3)**. Because the technology was opaque, even though participants wanted to stop sharing their accounts, they could not tell if they were successfully logged out of an account on all places where the account was used.

   Recommendation: Service providers could support users in these tasks by displaying all the devices that have accessed the account recently or since the last password change and allowing the user to end account access for some devices. The account could also be designed to allow the primary user to label devices to identify the devices accessing the account easily.

   We also recommend that users be able to give fine-grained permissions rather than all-or-nothing access to their personal content. Social networking sites could design personal accounts to enable users to give other users the right to view and/or modify certain parts of their personal content. This could include being able to view messages, reply to messages, and make posts on the shared accounts. To end the sharing of the accounts, the primary user would remove the permissions of the secondary user(s) in the account settings.

   Further, users could also be allowed to set a duration for how long they want to remain logged in. If users do not select this option, then they are automatically logged out of that device after a set time. While a "Keep me logged in" option is available on some accounts, we suggest that developers make it available on all online accounts with the option to specify how long the user remains logged in.

7.1.2 Anonymity

(the ability to hide one's true identity when using shared accounts)

The risk of an account being hijacked by a secondary user (see Section 2.3). The anonymity characteristic makes it easier for the secondary user to hide their true identity even after having compromised a previously shared account.

Recommendation: Support granting of fine-grained permissions to secondary users as described above. Further, ensure that the primary user always stays in control of the account. Sometimes the primary users face a "racing problem" when

Figure 7.2: Figure showing the current and ideal technological dimensions for *Anonymity* in shared accounts

ending password-based sharing. When account sharing ends, whoever resets the account password first wins the race by taking control of the account. We suggest that service providers could make sure that the primary user keeps control of the account independently of the actions by the secondary user(s).

7.1.3 Boundlessness

(refers to the lack of geographical barriers. Technology is not confined to a particular space or geographical location.)

The risk of an account being hijacked by a secondary user (see Section 2.3). The boundlessness characteristic accentuates this challenge by making it easier for the secondary user to abuse or continue an abuse even if the primary user has physically moved on from the relationship.

Recommendation: Same as above.

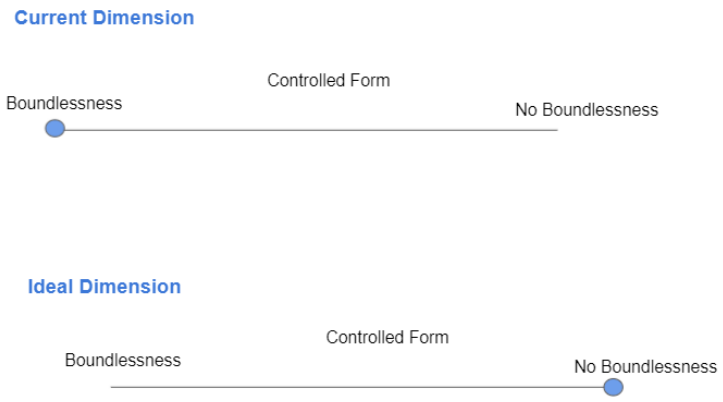

Figure 7.3: Figure showing the current and ideal technological dimensions for *Boundlessness* in shared accounts

7.2 Technological Dimensions related to the Security and Privacy Challenges of Mass Telecommuting (Chapter 3)

Technology: *Telecommuting devices.*
Users: *Workers.* Note that for this discussion, we chose workers. Another user type could be employers. For this type of user, there may be other security and privacy challenges and related technological dimensions.
Action: *Do organizational assigned work.*

7.2.1 Anonymity

(the ability to hide one's true identity while telecommuting)

The tension between professionalism and privacy on video calls (see Section 3.5.2). While technology provides anonymity, however, telecommuting leads to situations where people are sometimes compelled to disclose their identity. For some people, their identity could be that they are a father of two, with a wife and a pet. Workers wanted a controlled form of anonymity. They want to control who saw their homes, children, pets, etc. while working from home.

Recommendation: We suggest technology support for alerting participants of video calls when screenshots are taken to help employees maintain awareness of

Figure 7.4: Figure showing the current and ideal technological dimensions for *Anonymity* in telecommuting

their privacy and anonymity violations and to deter abuse of such capabilities by others.

7.2.2 Malleability

(the ease with which digital content can be tampered with)

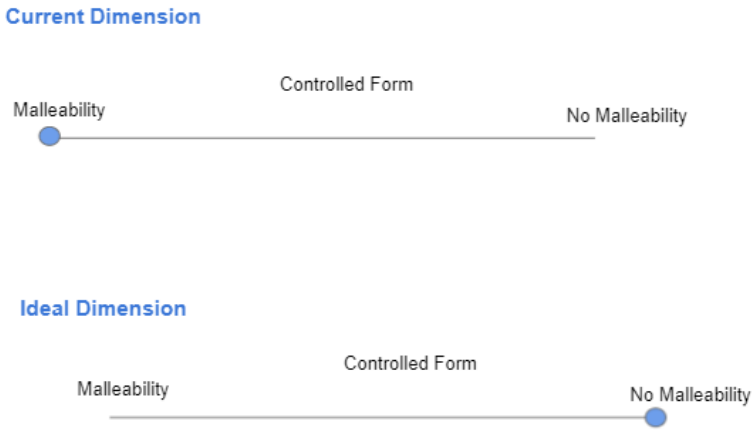

Figure 7.5: Figure showing the current and ideal technological dimensions for *Malleability* in telecommuting

Unauthorized people controlling participants' computer remotely (see Sec-

tion 3.5.2). Workers were afraid that giving their clients remote access to their computers while telecommuting could lead to unauthorized access and tampering with their personal and work data.

7.2.3 Opaqueness

(refers to a system with contents that are mysterious to the user. In our case, the system is telecommuting devices)

Figure 7.6: Figure showing the current and ideal technological dimensions for *Opaqueness* in telecommuting

Challenges with using the technology (see Section 3.5.4). As seen in Section 3.5.4, in some cases, challenges with using technology were because the technology was opaque for users to understand.

Recommendation: Efforts should be geared towards making technological solutions more transparent to use. Betzing et al., for instance, did a study with mobile device users to test the impact of transparency on how much access mobile devices have to users' personal information. The authors discovered that transparency about mobile device practices helped improve users' comprehension of data practices and policies [20]. Transparency could be achieved by making solutions more intuitive to use and reduce the learning curve needed to use the technology [106].

Improving users' mental models could help them better understand the technology. One main goal of the usable security and privacy community is to improve users' mental models about various technologies to avoid dangerous errors [275].

Similarly, the community could research the development of better mental models for users to help them make informed decisions about technological evidence. For instance, a research group at Carnegie Melon University is developing IoT security and privacy labels to improve people's mental models about their IoT devices [327]. Similar labels could be used to improve users' mental models about technology.

7.2.4 Covertness

(the trait of technology that enables one to operate technology in a particular location without the knowledge of the impacted individuals)

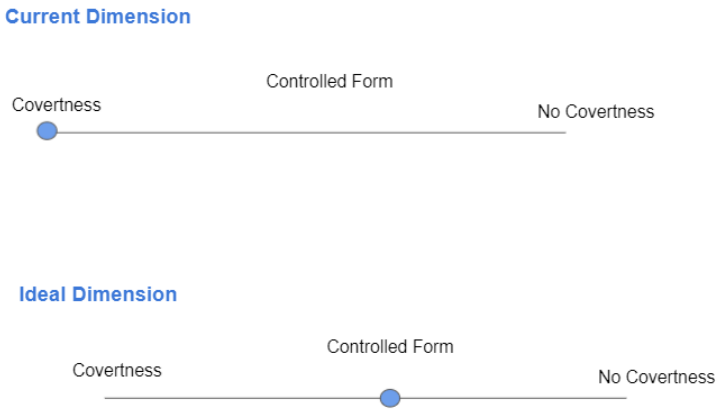

Figure 7.7: Figure showing the current and ideal technological dimensions for *Covertness* in telecommuting

Employee's location could be traced (see Section 3.5.3). Even though it may be impossible to trace work calls made from home, this fear could be because technology can be in use at a location without the knowledge of the impacted individual. It was possible for the 'tracing' to be happening without the knowledge of the participant.

Recommendation: Employers can put measures in place to manage the safety of the telecommuters, and their households Organizations need to be sensitive to the employees' physical security and consider the reality that different employees live in neighborhoods with varying safety levels. Organizations can be mindful of this threat and manage it as part of their policies or processes for handling work

from home. For long-term (and full-time) telecommuting, employers could consider setting up home alarm systems for their employees. The employers could also look into setting up work hubs where the organization's devices could be set up, and the employee's safety is protected.

Further, employers can educate employees about security measures at the work hub to allay their fears.

We also suggest that organizations provide clear guidelines on managing the home-work environment to optimize employees' physical safety. For instance, similar to on-site organizational security measures, employers could develop processes for physical security while telecommuting, such as help lines or safety routines that employees could use.

7.3 Technological Dimensions related to the Security and Privacy Challenges of Using Technological Solution to Report Sexual Assault (Chapter 4)

Technology: *Online third-party reporting systems (O-TPRS).*
Users: *Survivors.* Note that for this discussion, we chose survivors. Other user types could be social workers and the police. For these types of users, there may be other security and privacy challenges and related technological dimensions.
Action: *Report a sexual assault incident.*

7.3.1 Opaqueness

(refers to a system with contents that are mysterious to the user. In our case, the system is O-TPRS)

1. **The insecurity of the internet-Fear of the unknown (see Section 4.4.1)**. Participants had the *fear of the unknown* when using O-TPRS. They perceived that the internet was too opaque and they did not know the internet as much as attackers did. Therefore, they were not keen on trusting and using an O-TPRS.

2. **Lack of competency with using technology (see Section 4.4.1)**. Similar to the above, participants believed the technology was too complex and vast to

Figure 7.8: Figure showing the current and ideal technological dimensions for *Opaqueness* in O-TPRS

understand.

Recommendation: Similar to previous suggestions, improving the survivors' mental model could help them better understand the technology. This improvement could be done through educational videos in the O-TPRS that explain how their sexual assault report will be stored and used and their level of control with using the system.

7.3.2 Covertness

(the trait of technology that enables one to operate technology in a particular location without the knowledge of the impacted individuals)

The insecurity of the internet-Fear of the unknown (see Section 4.4.1). Because of the covertness characteristic, participants perceived that the perpetrators could see their sexual assault information without the survivor knowing, and this could lead to re-victimization from the perpetrators.

Recommendation: Same as above

7.3.3 Publicness

(information kept on the internet is public. Public characteristic refer to publicly available information created when a person uses technology)

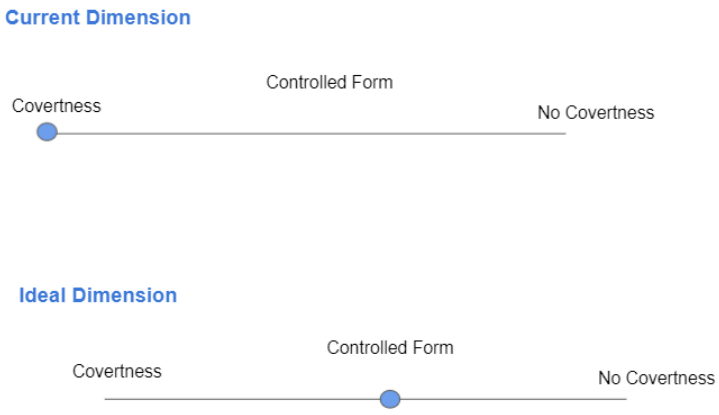

Figure 7.9: Figure showing the current and ideal technological dimensions for *Covertness* in O-TPRS

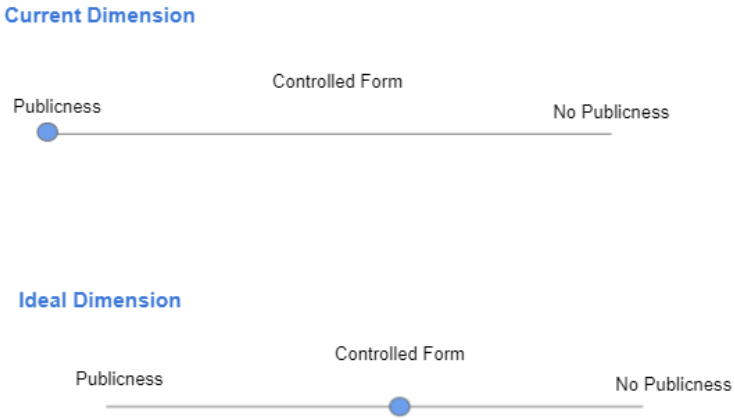

Figure 7.10: Figure showing the current and ideal technological dimensions for *Publicness* in O-TPRS

The traceability of online reporting (see Section 4.4.1). Participants were concerned that the information kept online was public and was no secret at all. Therefore whatever information they kept on the O-TPRS could be traced back to them by their perpetrators.

Lack of control (see Section 4.4.1). Similarly, survivors were concerned that they had no control over the information kept online, making the information public. Survivors were concerned that their sexual assault information would be made

public once it was online.

Recommendation: If a sexual assault survivor lives in an unconducive situation, having an O-TPRS app on their phones, even in disguise, may bring harm to the survivor. An option to hide survivors' online history could be for survivors to access the O-TPRS only in incognito mode or through a Tor browser. Note, however, that these designs require a certain level of familiarity with technology, and survivors may not find such designs usable. Further, incognito mode won't help in a scenario when the perpetrator has installed a key logger or is eavesdropping the traffic between the survivor's computer and the internet [1].

Another option could be the inclusion of a process to verify a survivor's identity on an O-TPRS. This verification process could be done through an authentication system. However, depending on the name supplied to the O-TPRS system, this design may not provide privacy because the presence of the app or website on a person's device may reveal to others that the person is a survivor.

7.4 Conclusion

As technology is taking the central stage in most of our relationships, investigating and addressing the security and privacy challenges that emerge from using technologies becomes of utmost importance and priority. We hope our design rubric can contribute to predicting and mitigating security and privacy concerns in existing and new technologies, and our dissertation as a whole can spur discussions in the research community on how existing challenges can be addressed.

Bibliography

[1] R. Abu-Salma and B. Livshits. Evaluating the end-user experience of private browsing mode. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pages 1–12, 2020. → pages 91, 134

[2] ACCESS. Sexual abuse. https://www.assaultcarecenter.org/en/sexual_abuse/, 2020. Accessed: 2019-02-26. → page 91

[3] A. Acquisti, L. Brandimarte, and G. Loewenstein. Privacy and human behavior in the age of information. *Science*, 347(6221):509–514, 2015. → page 60

[4] A. Adams-Prassl, T. Boneva, M. Golin, and C. Rauh. Work tasks that can be done from home: Evidence on variation within & across occupations and industries. *CEPR Discussion Paper No. DP14901*, 2020. → page 5

[5] C. Adeirnan, D. Jenkins, and S. Kemmis. Rethinking case study: notes from the second cambridge conference'in h simon. *Towards a Science of the Singular*, 1980. → page 97

[6] I. Altman. The environment and social behavior: privacy, personal space, territory, and crowding. *ERIC*, 1975. → pages 60, 103

[7] J. Ameriks, J. Briggs, A. Caplin, M. Lee, M. D. Shapiro, and C. Tonetti. Older americans would work longer if jobs were flexible. *American Economic Journal: Macroeconomics*, 12(1):174–209, 2020. → page 5

[8] Apple. Apple support. http://support.apple.com/en-ca/HT204976, 2019. Accessed: 2019-12-23. → page 34

[9] I. Araujo and I. Araujo. Developing trust in internet commerce. In *Proceedings of the 2003 conference of the Centre for Advanced Studies on Collaborative research*, pages 1–15, 2003. → page 79

[10] B. Arief, K. P. Coopamootoo, M. Emms, and A. van Moorsel. Sensible privacy: how we can protect domestic violence survivors without facilitating misuse. In *Proceedings of the 13th Workshop on Privacy in the Electronic Society*, pages 201–204, 2014. → page 115

[11] B. Arief, K. P. Coopamootoo, M. Emms, and A. van Moorsel. Sensible privacy: How we can protect domestic violence survivors without facilitating misuse. In *Proceedings of the 13th Workshop on Privacy in the Electronic Society*, pages 201–204, 2014. → pages 90, 91

[12] A. Attrill-Smith and C. Wesson. The psychology of cybercrime. *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, pages 653–678, 2020. → pages 111, 117

[13] J. E. Bahner, A.-D. Hüper, and D. Manzey. Misuse of automated decision aids: Complacency, automation bias and the impact of training experience. *International Journal of Human-Computer Studies*, 66(9):688–699, 2008. → page 72

[14] S. Banjo, L. Yap, C. Murphy, and V. Chan. Coronavirus forces world's largest work-from-home experiment. https://www.bloomberg.com/news/articles/2020-02-02/coronavirus-forces-world-s-largest-work-from-home-experiment, 2020. Accessed: 2020-09-11. → page 4

[15] T. Bank. TD bank joint account. http://tdbank.intelliresponse.com/?requestType=NormalRequest&source=3&question=How+do+I+open+or+close+a+joint+account, 2019. Accessed: 2019-12-23. → page 30

[16] J. Barkley, K. Beznosov, and J. Uppal. Supporting relationships in access control using role based access control. In *Proceedings of the fourth ACM workshop on Role-based access control*, pages 55–65. ACM, 1999. → page 34

[17] D. W. Bates, M. Cohen, L. L. Leape, J. M. Overhage, M. M. Shabot, and T. Sheridan. Reducing the frequency of errors in medicine using information technology. *Journal of the American Medical Informatics Association*, 8(4):299–308, 2001. → page 1

[18] A. Beautement, M. A. Sasse, and M. Wonham. The compliance budget: managing security behaviour in organisations. In *Proceedings of the 2008*

New Security Paradigms Workshop, pages 47–58. ACM, 2009. → pages 28, 32

[19] L.-K. Bernstein. Investigating and prosecuting swatting crimes. *US Att'ys Bull.*, 64:51, 2016. → page 94

[20] J. H. Betzing, M. Tietz, J. vom Brocke, and J. Becker. The impact of transparency on mobile privacy decision making. *Electronic Markets*, 30 (3):607–625, 2020. → page 129

[21] P. Bischoff. Nearly Half of Netflix Subscribers Share their Account Passwords. https://www.comparitech.com/blog/vpn-privacy/sharing-netflix-passwords/, March 2019. Accessed: 2019-12-16. → page 27

[22] C. Black. Global threat report extended enterprise under threat. https://www.carbonblack.com/wp-content/uploads/VMWCB-Report-GTR-Extended-Enterprise-Under-Threat-Global.pdf, 2020. Accessed: 2020-09-11. → pages 4, 5, 63

[23] N. Bloom. The bright future of working from home. https://siepr.stanford.edu/research/publications/bright-future-working-home, 2020. Accessed: 2020-09-11. → page 4

[24] N. Bloom. How working from home works out. https://siepr.stanford.edu/research/publications/how-working-home-works-out, 2020. Accessed: 2020-09-11. → page 4

[25] N. Bloom, J. Liang, J. Roberts, and Z. J. Ying. Does working from home work? evidence from a chinese experiment. *The Quarterly Journal of Economics*, 130(1):165–218, 2015. → page 5

[26] N. Bluett-Boyd, B. Fileborn, A. Quadara, and A. Moore. The role of emerging communication technologies in experiences of sexual violence: A new legal frontier? *Journal of the Home Economics Institute of Australia*, 20(2):25–29, 2013. → pages 113, 114, 115, 116, 117, 118, 119, 182, 183, 184

[27] J. M. Blythe and S. D. Johnson. A systematic review of crime facilitated by the consumer internet of things. *Security Journal*, pages 1–29, 2019. → pages 111, 116, 119

[28] J. Bonneau, C. Herley, P. C. Van Oorschot, and F. Stajano. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *2012 IEEE Symposium on Security and Privacy*, pages 553–567. IEEE, 2012. → page 103

[29] E. Borrajo, M. Gámez-Guadix, and E. Calvete. Cyber dating abuse: Prevalence, context, and relationship with offline dating aggression. *Psychological reports*, 116(2):565–585, 2015. → pages 111, 113

[30] V. Bouche et al. A report on the use of technology to recruit, groom and sell domestic minor sex trafficking victims. *Thorn*, 2015. → page 116

[31] S. Boulevard. Best practices: 6 physical security measures every company needs. https://securityboulevard.com/2019/03/best-practices-6-physical-security-measures-every-company-needs/, 2019. Accessed: 2021-02-1. → page 57

[32] D. Bourgeois and D. T. Bourgeois. Chapter 5: Networking and communication. https://bus206.pressbooks.com/chapter/chapter-5-networking-and-communication/, 2021. Accessed: 2021-04-15. → pages 2, 106

[33] D. Boyd. Taken out of context: American teen sociality in networked publics. *Available at SSRN 1344756*, 2008. → page 60

[34] S. Brennan and A. Taylor-Butts. *Sexual assault in Canada, 2004 and 2007*. Canadian Centre for Justice Statistics Ottawa, Ontario: Statistics Canada, 2008. → page 67

[35] T. Browser. Defend yourself. protect yourself against tracking, surveillance, and censorship. https://www.torproject.org/download/, 2020. Accessed: 2019-02-27. → page 91

[36] J. Bryce. Online sexual exploitation of children and young people. *Handbook of internet crime*, pages 320–342, 2010. → pages 115, 183

[37] A. Buchenscheit, B. Könings, A. Neubert, F. Schaub, M. Schneider, and F. Kargl. Privacy implications of presence sharing in mobile messaging applications. In *Proceedings of the 13th international conference on mobile and ubiquitous multimedia*, pages 20–29, 2014. → page 60

[38] C. M. Bullock and M. Beckson. Male victims of sexual assault: Phenomenology, psychology, physiology. *Journal of the American*

Academy of Psychiatry and the Law Online, 39(2):197–205, 2011. → page 67

[39] E. Business. Identity theft vs impersonation: How are they two different? https://www.eubusiness.com/focus/identity-theft-vs-impersonation-how-are-they-two-different, 2021. Accessed: 2022-02-15. → pages xv, 120

[40] C. Califonia. Cohousing califonia. https://www.calcoho.org, 2021. Accessed: 2021-02-24. → page 62

[41] C. Calvert and J. Brown. Video voyeurism, privacy, and the internet: Exposing peeping toms in cyberspce. *Cardozo Arts & Ent. LJ*, 18:469, 2000. → page 118

[42] B. C. Canada. British Columbia third party reporting protocol. https://endingviolence.org/wp-content/uploads/2019/10/TPR-Guidebook-2.0-July-2019.pdf, 2019. Accessed: 2019-02-26. → page 67

[43] B. C. Canada. Third party reporting for victims of sexual offences. https://www2.gov.bc.ca/gov/content/justice/criminal-justice/bcs-criminal-justice-system/reporting-a-crime/victim-or-witness-to-crime/third-party-reporting-for-victims-of-sexual-offences, 2020. Accessed: 2019-02-26. → pages 66, 67, 69, 70

[44] S. Canada. Retirement age by class of worker. https://www150.statcan.gc.ca/t1/tbl1/en/tv.action?pid=1410006001, 2020. Accessed: 2020-09-11. → page 54

[45] L. F. Cardoso, S. B. Sorenson, O. Webb, and S. Landers. Recent and emerging technologies: Implications for women's safety. *Technology in Society*, 58:101108, 2019. → page 111

[46] L. Carter and F. Bélanger. The utilization of e-government services: Citizen trust, innovation and acceptance factors. *Information systems journal*, 15(1):5–25, 2005. → page 93

[47] CBC. RCMP looks to expand third-party reporting for sexual assault cases. https://www.cbc.ca/news/politics/rcmp-sexual-assault-reporting-1.4402828, 2017. Accessed: 2019-06-27. → page 67

[48] CBC. Shopify permanently moves to work-from-home model. https://www.cbc.ca/news/canada/ottawa/shopify-pandemic-staff-ottawa-1.5578614, 2020. Accessed: 2021-01-18. → pages 5, 56, 63

[49] P. R. Center. Password management and mobile security. http://www.pewinternet.org/2017/01/26/2-password-management-and-mobile-security, January 2017. Accessed: 2019-02-27. → page 4

[50] D. Chaffey. Global social media statistics research summary 2021. https://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/, 2021. Accessed: 2020-09-16. → page 1

[51] E. Y. Chan and N. U. Saqib. Privacy concerns can explain unwillingness to download and use contact tracing apps when covid-19 concerns are high. *Computers in Human Behavior*, 119:106718, 2021. → page 99

[52] R. Chatterjee, P. Doerfler, H. Orgad, S. Havron, J. Palmer, D. Freed, K. Levy, N. Dell, D. McCoy, and T. Ristenpart. The spyware used in intimate partner violence. In *2018 IEEE Symposium on Security and Privacy (SP)*, pages 441–458. IEEE, 2018. → pages 110, 111

[53] C. Chen, N. Dell, and F. Roesner. Computer security and privacy in the interactions between victim service providers and human trafficking survivors. In *28th {USENIX} Security Symposium ({USENIX} Security 19)*, pages 89–104, 2019. → page 119

[54] D. Chen, S. Kalra, D. Irwin, P. Shenoy, and J. Albrecht. Preventing occupancy detection from smart meters. *IEEE Transactions on Smart Grid*, 6(5):2426–2434, 2015. → page 111

[55] Y. Chen and S. E. Ullman. Women's reporting of sexual and physical assaults to police in the national violence against women survey. *Violence Against Women*, 16(3):262–279, 2010. → page 6

[56] K.-K. R. Choo and A. I. of Criminology. *Online child grooming: A literature review on the misuse of social networking sites for grooming children for sexual offences*, volume 103. Australian Institute of Criminology Canberra, 2009. → pages 116, 118, 182

[57] P. Choudhury, C. Foroughi, and B. Z. Larson. Work-from-anywhere: The productivity effects of geographic flexibility. In *Academy of Management Proceedings*, volume 42, page 21199. Academy of Management Briarcliff Manor, NY 10510, 2020. → page 5

[58] G. Chrome. Browse in private. https://support.google.com/chrome/answer/95464?co=

GENIE.Platform%3DDesktop&hl=en, 2020. Accessed: 2019-02-27. → page 91

[59] L. Chu. Why would i adopt a smart speaker?: Consumers' intention to adopt smart speakers in smart home environment. Master's thesis, University of Twente, 2019. → page 99

[60] D. K. Citron. *Hate crimes in cyberspace*. Harvard University Press, 2014. → pages 115, 118

[61] K. Clarey. In the next decade, half of facebook's workforce could be remote. https://www.hrdive.com/news/facebook-remote-workforce-zuckerberg-announcement/578578/, 2020. Accessed: 2021-01-18. → pages 5, 56, 63

[62] F. Clear and K. Dickson. Teleworking practice in small and medium-sized firms: management style and worker autonomy. *New Technology, Work and Employment*, 20(3):218–233, 2005. → page 38

[63] CNBC. User Agreement. https://www.cnbc.com/2018/08/19/millennials-are-going-to-extreme-lengths-to-share-streaming-passwords-.html, August 2018. Accessed: 2019-02-28. → page 32

[64] C. Cobb, L. Simko, T. Kohno, and A. Hiniker. A privacy-focused systematic analysis of online status indicators. *Proceedings on Privacy Enhancing Technologies*, 2020(3):384–403, 2020. → page 60

[65] D. Cohen and B. Crabtree. Qualitative research guidelines project. http://www.qualres.org/, 2006. → pages 16, 41, 74, 97

[66] M. Cohen. Technology and relationships: The pros and cons. https://www.webmd.com/healthy-aging/features/tech-affects-relationships#1, 2016. Accessed: 2020-09-16. → page 2

[67] R. Cohen-Almagor. Online child sex offenders: Challenges and counter-measures. *The Howard Journal of Criminal Justice*, 52(2): 190–215, 2013. → pages 114, 116, 117, 118

[68] M. . Company. How covid-19 has pushed companies over the technology tipping point—and transformed business forever. https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/how-covid-19-has-pushed-companies-over-the-technology-tipping-point-and-transformed-business-forever, 2021. Accessed: 2020-09-16. → page 2

[69] R. E. Constantino, B. Braxter, D. Ren, J. D. Burroughs, W. M. Doswell, L. Wu, J. G. Hwang, M. L. Klem, J. B. Joshi, and W. B. Greene. Comparing online with face-to-face helpp intervention in women experiencing intimate partner violence. *Issues in mental health nursing*, 36 (6):430–438, 2015. → page 111

[70] T. Conversation. How to digitally disentangle after a break up, some new rules. http://theconversation.com/how-to-digitally-disentangle-after-a-break-up-some-new-rules-90592, February 2018. Accessed: 2019-02-27. → pages 4, 11

[71] A. Cotter. *Sexual misconduct in the Canadian Armed Forces, 2016*. Statistics Canada, 2016. → page 67

[72] A. Cotter and P. Beaupré. Police-reported sexual offences against children and youth in canada, 2012. *Juristat: Canadian Centre for Justice Statistics*, page 1, 2014. → page 67

[73] D. Couch, P. Liamputtong, and M. Pitts. What are the real and perceived risks and dangers of online dating? Perspectives from online daters: Health risks in the media. *Health, Risk & Society*, 14(7-8):697–714, 2012. → page 6

[74] C. Cross, M. Dragiewicz, and K. Richards. Understanding romance fraud: Insights from domestic violence research. *The British Journal of Criminology*, 58(6):1303–1322, 2018. → page 115

[75] B. Cybulska. Sexual assault: Key issues. *Journal of the Royal Society of Medicine*, 100(7):321–324, 2007. → pages 6, 67

[76] E. L. Davies. *The lived experiences of individuals who have been technologically stalked by a past intimate: a hermeneutic phenomenological study through a Communication Privacy Management Theory lens*. PhD thesis, University of Missouri–Columbia, 2013. → page 112

[77] J. P. Dimond, C. Fiesler, and A. S. Bruckman. Domestic violence and information communication technologies. *Interacting with computers*, 23 (5):413–421, 2011. → pages 113, 114

[78] D. Dodd-McCue and A. Tartaglia. Self-report response bias: Learning how to live with its diagnosis in chaplaincy research. *Chaplaincy Today*, 26(1): 2–8, 2010. → page 121

[79] D. Dodd-McCue and A. Tartaglia. Self-report response bias: Learning how to live with its diagnosis in chaplaincy research. *Chaplaincy Today*, 26(1): 2–8, 2010. → pages 26, 54, 88

[80] A. Dodge. Digitizing rape culture: Online sexual violence and the power of the digital photograph. *Crime, media, culture*, 12(1):65–82, 2016. → pages 117, 118

[81] N. Doria, C. Ausman, S. Wilson, A. Consalvo, J. Sinno, and M. Numer. Women's experiences of safety apps for sexualized violence: A narrative scoping review, 2020. → page 111

[82] N. Döring and S. Pöschl. Nonverbal cues in mobile phone text messages: The effects of chronemics and proxemics. In *The reconstruction of space and time*, pages 109–135. Routledge, 2017. → page 1

[83] J. R. Douceur. The Sybil attack. In *International workshop on peer-to-peer systems*, pages 251–260. Springer, 2002. → page 93

[84] H. Douglas, B. A. Harris, and M. Dragiewicz. Technology-facilitated domestic and family violence: Women's experiences. *The British Journal of Criminology*, 59(3):551–570, 2019. → pages 111, 113, 116, 118

[85] M. Dragiewicz, J. Burgess, A. Matamoros-Fernández, M. Salter, N. P. Suzor, D. Woodlock, and B. Harris. Technology facilitated coercive control: Domestic violence and the competing roles of digital media platforms. *Feminist Media Studies*, 18(4):609–625, 2018. → pages 112, 114, 117, 118

[86] C. B. Draucker and D. S. Martsolf. The role of electronic communication technology in adolescent dating violence. *Journal of Child and Adolescent Psychiatric Nursing*, 23(3):133–142, 2010. → pages 111, 117

[87] K. Duerksen. *Technological intimate partner violence: victim impacts and technological perpetration factors*. PhD thesis, University of Victoria, 2018. → page 111

[88] J. A. Dunlap. Intimate terrorism and technology: There's and app for that. *U. Mass. L. Rev.*, 7:10, 2012. → pages 113, 117, 185

[89] J. J. Eckstein and C. Danbury. What is violence now?: A grounded theory approach to conceptualizing technology-mediated abuse (tma) as spatial and participatory. *The Electronic Journal of Communication*, 29(3-4), 2020. → page 111

[90] S. Egelman, A. Brush, and K. M. Inkpen. Family accounts: a new paradigm for user accounts within the home environment. In *Proceedings of the 2008 ACM conference on Computer supported cooperative work*, pages 669–678. ACM, 2008. → page 13

[91] J. Elliott and K. McCartan. The reality of trafficked people's access to technology. *The Journal of Criminal Law*, 77(3):255–273, 2013. → page 117

[92] M. Eneman, A. A. Gillespie, C. S. Bernd, and B. Stahl. Technology and sexual abuse: A critical review of an internet grooming case. In *International Conference on Information Systems*, pages 1–17. Citeseer, 2010. → pages 114, 116, 117

[93] G. Evangelakos. Keeping critical assets safe when teleworking is the new norm. *Network Security*, 2020(6):11–14, 2020. → page 5

[94] Facebook. Using facebook-tagging. https://www.facebook.com/help/tagging, 2021. Accessed: 2021-03-30. → page 113

[95] J. Fairbairn and D. Spencer. Virtualized violence and anonymous juries: Unpacking steubenville's "big red" sexual assault case and the role of social media. *Feminist criminology*, 13(5):477–497, 2018. → page 184

[96] C. Ferrán-Urdaneta and J. Storck. Truth or deception: The impact of videoconferencing on job interviews. 1997. → page 1

[97] J. Finn and T. Atkinson. Promoting the safe and strategic use of technology for victims of intimate partner violence: Evaluation of the technology safety project. *Journal of Family Violence*, 24(1):53–59, 2009. → page 110

[98] S. M. Flanagan, S. Greenfield, J. Coad, and S. Neilson. An exploration of the data collection methods utilised with children, teenagers and young people (ctyps). *BMC research notes*, 8(1):61, 2015. → page 75

[99] D. Florencio and C. Herley. A large-scale study of web password habits. In *Proceedings of the 16th international conference on World Wide Web*, pages 657–666. ACM, 2007. → page 33

[100] A. Flynn and N. Henry. Image-based sexual abuse: an australian reflection. *Women & Criminal Justice*, pages 1–14, 2019. → page 117

[101] A. Flynn and N. Henry. Image-based sexual abuse: an australian reflection. *Women & Criminal Justice*, pages 1–14, 2019. → page 118

[102] T. S. for Abused Women. Social media & technology abuse. http://tearmann.ca/about-abuse/digital-abuse/, 2015. Accessed: 2020-09-16. → page 2

[103] M. T. Ford, C. P. Cerasoli, J. A. Higgins, and A. L. Decesare. Relationships between psychological, physical, and behavioural health and work performance: A review and meta-analysis. *Work & Stress*, 25(3):185–204, 2011. → page 56

[104] P. Forde and A. Patterson. *Paedophile internet activity*. Australian Institute of Criminology Canberra, 1998. → page 109

[105] S. G. Forrestal, A. V. D'Angelo, L. K. Vogel, et al. Considerations for and lessons learned from online, synchronous focus groups. *Survey Practice*, 8 (2):1–8, 2015. → page 77

[106] I. D. Foundation. Intuitive design. https://www.interaction-design.org/literature/topics/intuitive-design, 2021. Accessed: 2021-04-14. → page 129

[107] C. Fraser, E. Olsen, K. Lee, C. Southworth, and S. Tucker. The new age of stalking: Technological implications for stalking. *Juvenile and family court journal*, 61(4):39–55, 2010. → pages 111, 112, 113, 115, 116, 183, 184

[108] D. Freed, J. Palmer, D. E. Minchala, K. Levy, T. Ristenpart, and N. Dell. Digital technologies and intimate partner violence: A qualitative analysis with multiple stakeholders. *Proceedings of the ACM on Human-Computer Interaction*, 1(CSCW):1–22, 2017. → pages 111, 116

[109] D. Freed, J. Palmer, D. E. Minchala, K. Levy, T. Ristenpart, and N. Dell. Digital technologies and intimate partner violence: A qualitative analysis with multiple stakeholders. *Proceedings of the ACM on Human-Computer Interaction*, 1(CSCW):46, 2017. → pages 14, 24

[110] D. Freed, J. Palmer, D. Minchala, K. Levy, T. Ristenpart, and N. Dell. "a stalker's paradise" how intimate partner abusers exploit technology. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, pages 1–13, 2018. → pages 111, 117, 185

[111] D. Freed, J. Palmer, D. Minchala, K. Levy, T. Ristenpart, and N. Dell. "A stalker's paradise" How intimate partner abusers exploit technology. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, pages 1–13, 2018. → page 90

[112] D. Freed, J. Palmer, D. Minchala, K. Levy, T. Ristenpart, and N. Dell. "a stalker's paradise": How intimate partner abusers exploit technology. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, page 667. ACM, 2018. → page 14

[113] D. Frome. Masked calling. https://www.twilio.com/docs/glossary/what-is-masked-calling, 2020. Accessed: 2020-01-07. → page 58

[114] M. P. Gallaher, B. R. Rowe, A. V. Rogozhin, and A. N. Link. Economic analysis of cyber security. Technical report, Research Triangle Inst (RTI) Research Triangle Park NC, 2006. → page 92

[115] D. Gefen, E. Karahanna, and D. W. Straub. Trust and TAM in online shopping: An integrated model. *MIS quarterly*, 27(1):51–90, 2003. → page 71

[116] A. A. Gillespie. Child protection on the internet-challenges for criminal law. *Child & Fam. LQ*, 14:411, 2002. → pages 114, 116

[117] R. Gillett. Intimate intrusions online: Studying the normalisation of abuse in dating apps. In *Women's Studies International Forum*, volume 69, pages 212–219. Elsevier, 2018. → page 111

[118] R. Gillett. Intimate intrusions online: Studying the normalisation of abuse in dating apps. In *Women's Studies International Forum*, volume 69, pages 212–219. Elsevier, 2018. → pages 111, 113

[119] N. Girvan. Power imbalances and development knowledge. 2007. → page 104

[120] R. Golden. Gartner: Over 80% of company leaders plan to permit remote work after pandemic. https://www.hrdive.com/news/gartner-over-80-of-company-leaders-plan-to-permit-remote-work-after-pande/581744/, 2020. Accessed: 2021-01-18. → pages 5, 63

[121] M. Graham, A. Milanowski, and J. Miller. Measuring and promoting inter-rater agreement of teacher and principal performance ratings. *Online Submission*, 2012. → page 18

[122] Greetly. Workplace security & access control - the fundamentals. https://www.greetly.com/blog/workplace-security-access-control-the-fundamentals, 2020. Accessed: 2021-02-1. → page 57

[123] V. Greiman and C. Bain. The emergence of cyber activity as a gateway to human trafficking. *Journal of Information Warfare*, 12(2):41–49, 2013. → page 111

[124] T. Guardian. From ghosting to oversharing: the new rules of breakups. https://www.theguardian.com/lifeandstyle/2018/nov/15/new-rules-of-breakups, 2018. Accessed: 2019-02-27. → page 27

[125] G. Guest, K. M. MacQueen, and E. E. Namey. *Applied thematic analysis*. Sage Publications, 2011. → pages 17, 42, 77

[126] G. Guest, K. M. MacQueen, and E. E. Namey. Introduction to applied thematic analysis. *Applied thematic analysis*, 3:20, 2012. → pages 7, 17, 41, 77

[127] V. M. Hamilton. *Human Relations : The Art and Science of Building Effective Relationships*. Prentice Hall, 2007. → page 2

[128] K. Hammarberg, M. Kirkman, and S. de Lacey. Qualitative research methods: When to use them and how to judge them. *Human reproduction*, 31(3):498–501, 2016. → page 73

[129] T. Hand, D. Chung, and M. Peters. *The use of information and communication technologies to coerce and control in domestic violence and following separation*. Australian Domestic and Family Violence Clearinghouse, UNSW Sydney, AU, 2009. → pages 111, 113, 117

[130] P. L. Hardré. When, how, and why do we trust technology too much? In *Emotions, Technology, and Behaviors*, pages 85–106. Elsevier, 2016. → pages 67, 72

[131] B. A. Harris. Technology and violence against women. In *The Emerald Handbook of Feminism, Criminology and Social Change*. Emerald Publishing Limited, 2020. → page 111

[132] B. A. Harris and D. Woodlock. Digital coercive control: Insights from two landmark domestic violence studies. *The British Journal of Criminology*, 59(3):530–550, 2019. → page 111

[133] B. A. Harris and D. Woodlock. Digital coercive control: Insights from two landmark domestic violence studies. *The British Journal of Criminology*, 59(3):530–550, 2019. → page 111

[134] I. Harris, Y. Wang, and H. Wang. Ict in multimodal transport and technological trends: Unleashing potential for the future. *International Journal of Production Economics*, 159:88–103, 2015. → page 1

[135] L. Hart and C. Mitchell. From spaces of sexual violence to sites of networked resistance: Re-imagining mobile and social media technologies. *Perspectives in Education*, 33(4):135–150, 2015. → pages 110, 111

[136] A.-W. Harzing. *The publish or perish book*. Tarma Software Research Pty Limited Melbourne, Australia, 2010. → pages 108, 121

[137] S. Havron, D. Freed, R. Chatterjee, D. McCoy, N. Dell, and T. Ristenpart. Clinical computer security for victims of intimate partner violence. In *28th {USENIX} Security Symposium ({USENIX} Security 19)*, pages 105–122, 2019. → pages 110, 112

[138] S. Havron, D. Freed, R. Chatterjee, D. McCoy, N. Dell, and T. Ristenpart. Clinical computer security for victims of intimate partner violence. In *28th {USENIX} Security Symposium ({USENIX} Security 19)*, pages 105–122, 2019. → page 111

[139] R. M. Hayes and M. Dragiewicz. Unsolicited dick pics: Erotica, exhibitionism or entitlement? In *Women's Studies International Forum*, volume 71, pages 114–120. Elsevier, 2018. → page 117

[140] M. B. Heinskou, M.-L. Skilbrei, and K. Stefansen. *Rape in the Nordic countries: Continuity and change*. Routledge, 2019. → page 117

[141] R. J. Heintzman. Confidence schemes and con games: Old games with new players. *FBI L. Enforcement Bull.*, 55:11, 1986. → page 115

[142] G. Helgesson, M. G. Hansson, J. Ludvigsson, and U. Swartling. Practical matters, rather than lack of trust, motivate non-participation in a long-term cohort trial. *Pediatric diabetes*, 10(6):408–412, 2009. → page 68

[143] M. A. Henderson. *Flimflam Man: How Con Games Work*. Paladin Press, 1985. → page 115

[144] N. Henry and A. Flynn. Image-based sexual abuse: A feminist criminological approach. *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, pages 1109–1130, 2020. → page 117

[145] N. Henry and A. Powell. The dark side of the virtual world. In *Preventing Sexual Violence*, pages 84–104. Springer, 2014. → page 81

[146] N. Henry and A. Powell. The dark side of the virtual world. In *Preventing Sexual Violence*, pages 84–104. Springer, 2014. → pages 111, 112, 114, 115

[147] N. Henry and A. Powell. Beyond the 'sext': Technology-facilitated sexual violence and harassment against adult women. *Australian & New Zealand Journal of Criminology*, 48(1):104–118, 2015. → page 116

[148] N. Henry and A. Powell. Beyond the 'sext': Technology-facilitated sexual violence and harassment against adult women. *Australian & New Zealand Journal of Criminology*, 48(1):104–118, 2015. → page 81

[149] N. Henry and A. Powell. Embodied harms: Gender, shame, and technology-facilitated sexual violence. *Violence against women*, 21(6): 758–779, 2015.

[150] N. Henry and A. Powell. Sexual violence in the digital age: The scope and limits of criminal law. *Social & Legal Studies*, 25(4):397–418, 2016. → page 81

[151] N. Henry and A. Powell. Technology-facilitated sexual violence: A literature review of empirical research. *Trauma, violence, & abuse*, 19(2): 195–208, 2018. → page 118

[152] N. Henry, A. Flynn, and A. Powell. Policing image-based sexual abuse: Stakeholder perspectives. *Police practice and research*, 19(6):565–581, 2018. → pages 117, 118

[153] N. Henry, A. Flynn, and A. Powell. *Responding to'revenge Pornography': Prevalence, Nature and Impacts*. Criminology Research Grants Program, Australian Institute of Criminology, 2019. → page 117

[154] C. Herley. So long, and no thanks for the externalities: the rational rejection of security advice by users. In *Proceedings of the 2009 workshop on New security paradigms workshop*, pages 133–144. ACM, 2009. → page 27

[155] D. Herron, W. Moncur, and E. van den Hoven. Digital decoupling and disentangling: towards design for romantic break up, 2017. → pages 15, 27

[156] K. R. Holladay and W. B. Hagedorn. The use of technology in sexual exploration among a rape culture youth. *Journal of Counseling Sexology &*

Sexual Wellness: Research, Practice, and Education, 1(2):3, 2019. → page 117

[157] T. J. Holt, K. R. Blevins, and N. Burkert. Considering the pedophile subculture online. *Sexual Abuse*, 22(1):3–24, 2010. → pages 115, 116

[158] R. Hoyle, S. Das, A. Kapadia, A. J. Lee, and K. Vaniea. Was my message read? privacy and signaling on facebook messenger. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, pages 3838–3842, 2017. → page 60

[159] D. M. Hughes. Trafficking in human beings in the european union: Gender, sexual exploitation, and digital communication technologies. *Sage Open*, 4 (4):2158244014553585, 2014. → pages 116, 118

[160] T. Hunt. The trouble with politicians sharing passwords. https://www.troyhunt.com/the-trouble-with-politicians-sharing-passwords/, 2017. Accessed: 2019-07-30. → page 4

[161] Huridocs. 5 steps to protect your data in case of computer theft. https://huridocs.org/2015/12/steps-to-protect-your-data-computer-theft/, 2015. Accessed: 2021-02-1. → page 57

[162] G. Hurlburt. "Good enough" security: The best we'll ever have. *Computer*, 49(7):98–101, 2016. → page 92

[163] C. F. S. Index. Survey: More than Half of Americans Are Using Shared Services Like Uber, Lyft and Airbnb. https://www.countryfinancial.com/en/about-us/newsroom/year2018/More-than-Half-of-Americans-Are-Using-Shared-Services.html, September 2018. Accessed: 2019-02-27. → page 4

[164] C. F. Institute. What are negative externalities? https://corporatefinanceinstitute.com/resources/knowledge/economics/negative-externalities/, 2021. Accessed: 2021-02-24. → page 57

[165] INTERPOL. Interpol report shows alarming rate of cyberattacks during covid-19. https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19, 2020. Accessed: 2021-01-18. → page 4

[166] M. Jacobs, H. Cramer, and L. Barkhuus. Caring about sharing: Couples' practices in single user device access, 2016. → pages 1, 4, 11, 13, 27, 30

[167] E. Jardine. *The Dark Web dilemma: Tor, anonymity and online policing*. Centre for International Governance Innovation and Chatham House, 2015. → page 91

[168] D. Jeslet, G. Sivaraman, M. Uma, K. Thangadurai, and M. Punithavalli. Survey on awareness and security issues in password management strategies. *IJCSNS*, 10(4), 2010. → page 27

[169] M. E. Kabay. Anonymity and pseudonymity in cyberspace: deindividuation, incivility and lawlessness versus freedom and privacy. In *Annual Conference of the European Institute for Computer Anti-virus Research (EICAR), Munich, Germany*, pages 16–8. Citeseer, 1998. → page 121

[170] T. E. Kadri. Networks of empathy. *Utah L. Rev.*, page 1075, 2020. → page 100

[171] J. J. Kaye. Self-reported password sharing strategies. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 2619–2622. ACM, 2011. → pages 21, 27

[172] J. Kelly. Twitter ceo jack dorsey tells employees they can work from home 'forever'—before you celebrate, there's a catch. https://www.forbes.com/sites/jackkelly/2020/05/13/twitter-ceo-jack-dorsey-tells-employees-they-can-work-from-home-forever-before-you-celebrate-theres-a-catch/?sh=771246c82e91, 2020. Accessed: 2021-01-18. → pages 5, 56, 63

[173] Y. Keshet. Recent escalations in cyberattacks in italy prove the coronavirus impact on cybersecurity – acting as a warning for cisos worldwide. https://www.cynet.com/blog/recent-escalation-in-cyberattacks-in-italy-prove-the-coronavirus-impact-on-cybersecurity-acting-as-a-warning-for-cisos-worldwide/, 2020. Accessed: 2020-09-11. → pages 5, 63

[174] S. Kintner. Preliminary report telework/telecommuting: Employers' perspectives and perspectives of service members and veterans with disabilities. *e-Networks in an Increasingly Volatile World*, page 204, 2006. → pages 38, 61

[175] Klaxos.com. LinkedIn Profile Writing Service. https://ca.linkedin.com/company/linkedin-profile-service, 2009. Accessed: 2019-02-28. → page 32

[176] J. A. Kloess, A. R. Beech, and L. Harkins. Online child sexual exploitation: Prevalence, process, and offender characteristics. *Trauma, Violence, & Abuse*, 15(2):126–139, 2014. → pages 113, 114, 115, 116, 117, 118

[177] G. M. Koien and V. A. Oleshchuk. *Aspects of Personal Privacy in Communications: Problems, Technology and Solutions*. River Publishers, 2013. → page 2

[178] S. Kostova, M. Dimitrova, V. Kaburlasos, E. Vrochidou, G. Papakostas, T. Pachidis, S. Saeva, M. Bonković, S. Kružić, T. Marasović, et al. Identifying needs of robotic and technological solutions for the classroom. In *2018 26th International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, pages 1–6. IEEE, 2018. → page 2

[179] D. R. Kuhn, M. C. Tracy, and S. E. Frankel. Security for telecommuting and broadband communications. *NIST Special Publication*, 800:46, 2002. → page 5

[180] D. Lamey. The evolution of technology:past, present and future. https://www.discovertec.com/blog/evolution-of-technology, 2018. Accessed: 2021-03-22. → page 116

[181] O. Languages. Perpetrator. https://languages.oup.com/google-dictionary-en/, 2021. Accessed: 2021-04-12. → page 107

[182] W. C. LEAF. We are here: Women's experiences of the barriers to reporting sexual assault. http://www.westcoastleaf.org/our-publications/we-are-here-womens-experiences-of-the-barriers-to-reporting-sexual-assault/, 2018. Accessed: 2019-06-27. → pages 66, 67

[183] M. Lee. Encrypting your laptop like you mean it. https://theintercept.com/2015/04/27/encrypting-laptop-like-mean/, 2021. Accessed: 2021-02-1. → page 57

[184] C. Lehmann. Privacy concerns hindering digital contact tracing. https://www.webmd.com/lung/news/20200928/privacy-concerns-hindering-digital-contact-tracing, 2019. Accessed: 2021-06-12. → page 99

[185] R. Leitão. Digital technologies and their role in intimate partner violence. In *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems*, pages 1–6, 2018. → pages 111, 112, 113

[186] R. Leitão. Anticipating smart home security and privacy threats with survivors of intimate partner abuse. In *Proceedings of the 2019 on Designing Interactive Systems Conference*, pages 527–539, 2019. → pages 111, 119

[187] R. Leitão. Technology-facilitated intimate partner abuse: a qualitative analysis of data from online domestic abuse forums. *Human–Computer Interaction*, pages 1–40, 2019. → pages 111, 119

[188] LinkedIn. User Agreement. https://www.linkedin.com/legal/user-agreement, May 2018. Accessed: 2019-02-28. → page 32

[189] H. Liu. When whispers enter the cloud: Evaluating technology to prevent and report sexual assault. *Harv. JL & Tech.*, 31:939, 2017. → pages 72, 82

[190] C. Logie, R. Alaggia, and M.-J. Rwigema. A social ecological approach to understanding correlates of lifetime sexual assault among sexual minority women in toronto, canada: Results from a cross-sectional internet-based survey. *Health education research*, 29(4):671–682, 2014. → pages 6, 67

[191] D. Lohrmann. 2020: The year the covid-19 crisis brought a cyber pandemic. https://www.govtech.com/blogs/lohrmann-on-cybersecurity/2020-the-year-the-covid-19-crisis-brought-a-cyber-pandemic.html, 2020. Accessed: 2021-01-18. → page 4

[192] I. Lopez-Neira, T. Patel, S. Parkin, G. Danezis, and L. Tanczer. 'internet of things': How abuse is getting smarter. *Safe – The Domestic Abuse Quarterly*, 63:22–26, 2019. → pages 110, 116

[193] H. Luce, S. Schrager, and V. Gilchrist. Sexual assault of women. *American family physician*, 81(4):489–495, 2010. → page 6

[194] H. Madeleine. How has technology changed - and changed us - in the past 20 years? https://www.weforum.org/agenda/2020/11/heres-how-technology-has-changed-and-changed-us-over-the-past-20-years/, 2020. Accessed: 2020-09-16. → page 1

[195] N. Mahapatra and A. Rai. Every cloud has a silver lining but. . . "pathways to seeking formal-help and south-asian immigrant women survivors of intimate partner violence". *Health care for women international*, 40(11): 1170–1196, 2019. → page 111

[196] L. Makeover. Order Your LinkedIn Makeover Today. https://www.linkedin-makeover.com/order-today/, 2019. Accessed: 2019-02-28. → page 32

[197] D. Marques, I. Muslukhov, T. Guerreiro, L. Carriço, and K. Beznosov. Snooping on mobile phones: Prevalence and trends. In *Twelfth Symposium on Usable Privacy and Security ({SOUPS} 2016)*, pages 159–174, 2016. → page 34

[198] D. Marques, T. Guerreiro, L. Carriço, I. Beschastnikh, and K. Beznosov. Vulnerability & blame: Making sense of unauthorized access to smartphones. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. ACM, 2019. → pages 27, 32, 34

[199] E. Martellozzo. *Online child sexual abuse: Grooming, policing and child protection in a multi-media world*. Routledge, 2013. → page 116

[200] C. L. Mason and S. Magnet. Surveillance studies and violence against women. *surveillance & society*, 10(2):105–118, 2012. → pages 111, 113

[201] T. Matthews, K. Liao, A. Turner, M. Berkovich, R. Reeder, and S. Consolvo. She'll just grab any device that's closer: A study of everyday device & account sharing in households, 2016. → pages 4, 11, 13, 27, 32, 34

[202] T. Matthews, K. O'Leary, A. Turner, M. Sleeper, J. P. Woelfer, M. Shelton, C. Manthorne, E. F. Churchill, and S. Consolvo. Stories from survivors: Privacy & security practices when coping with intimate partner abuse. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, pages 2189–2201. ACM, 2017. → pages 14, 24, 110, 111, 113

[203] L. McAllister, A. Magee, and B. Hale. Women, e-waste, and technological solutions to climate change. *Health & Hum. Rts. J.*, 16:166, 2014. → page 1

[204] K. McCartan and R. McAlister. Mobile phone technology and sexual abuse. *Information & Communications Technology Law*, 21(3):257–268, 2012. → pages 114, 115, 116, 184

[205] J. M. McCarthy, J. P. Trougakos, and B. H. Cheng. Are anxious workers less productive workers? it depends on the quality of social exchange. *Journal of Applied Psychology*, 101(2):279, 2016. → page 56

[206] C. McGlynn, E. Rackley, and R. Houghton. Beyond 'revenge porn': The continuum of image-based sexual abuse. *Feminist Legal Studies*, 25(1): 25–46, 2017. → page 117

[207] D. H. McKnight, M. Carter, J. B. Thatcher, and P. F. Clay. Trust in a specific technology: An investigation of its components and measures. *ACM Transactions on management information systems (TMIS)*, 2(2): 12–32, 2011. → pages 71, 93

[208] A. M. Medrano-Gil, S. de los Ríos Pérez, G. Fico, J. B. Montalvá Colomer, G. Cea Sáncez, M. F. Cabrera-Umpierrez, and M. T. Arredondo Waldmeyer. Definition of technological solutions based on the internet of things and smart cities paradigms for active and healthy ageing through cocreation. *Wireless Communications and Mobile Computing*, 2018, 2018. → page 1

[209] G. Meet. Change your background in google meet. https://support.google.com/meet/answer/10058482?co=GENIE.Platform%3DDesktop&hl=en&oco=1#zippy=%2Cwhy-dont-i-have-the-change-background-option, 2021. Accessed: 2021-02-19. → page 45

[210] J. Messing, M. Bagwell-Gray, M. L. Brown, A. Kappas, and A. Durfee. Intersections of stalking and technology-based abuse: Emerging definitions, conceptualization, and measurement. *Journal of family violence*, pages 1–12, 2020. → page 111

[211] E. Minaya. 4,000% increase in ransomware emails during covid-19. https://www.nationalobserver.com/2020/04/14/news/4000-increase-ransomware-emails-during-covid-19?utm_source=National+Observer&utm_campaign=71c5787b54-EMAIL_CAMPAIGN_2020_04_14_12_21&utm_medium=email&utm_term=0_cacd0f141f-71c5787b54-276991505, 2020. Accessed: 2020-09-11. → pages 5, 63

[212] E. Minaya. Cfos plan to permanently shift significant numbers of employees to work remotely — survey. https://www.forbes.com/sites/ezequielminaya/2020/04/03/cfos-plan-to-permanently-shift-significant-numbers-of-employees-to-work-remotely---survey/#11bc806575b2, 2020. Accessed: 2020-09-11. → pages 4, 63

[213] K. J. Mitchell and d. boyd. Understanding the role of technology in the commercial sexual exploitation of children: the perspective of law

enforcement. *Crimes against Children Research Center*, 2014. → pages 115, 117, 118

[214] K. J. Mitchell, D. Finkelhor, L. M. Jones, and J. Wolak. Use of social networking sites in online sex crimes against minors: An examination of national incidence and means of utilization. *Journal of Adolescent Health*, 47(2):183–190, 2010. → pages 114, 117

[215] K. J. Mitchell, D. Finkelhor, L. M. Jones, and J. Wolak. Use of social networking sites in online sex crimes against minors: An examination of national incidence and means of utilization. *Journal of Adolescent Health*, 47(2):183–190, 2010. → page 113

[216] K. J. Mitchell, L. M. Jones, D. Finkelhor, and J. Wolak. Internet-facilitated commercial sexual exploitation of children: Findings from a nationally representative sample of law enforcement agencies in the united states. *Sexual Abuse*, 23(1):43–71, 2011. → page 115

[217] K. J. Mitchell, L. M. Jones, D. Finkelhor, and J. Wolak. Internet-facilitated commercial sexual exploitation of children: Findings from a nationally representative sample of law enforcement agencies in the united states. *Sexual Abuse*, 23(1):43–71, 2011. → pages 115, 116, 117, 183

[218] W. Moncur, L. Gibson, and D. Herron. The role of digital technologies during relationship breakdowns, 2016. → pages 4, 11, 15, 26, 27

[219] E. Montague and O. Asan. Trust in technology-mediated collaborative health encounters: Constructing trust in passive user interactions with technologies. *Ergonomics*, 55(7):752–761, 2012. → page 72

[220] D. L. Morgan. *Focus groups as qualitative research*, volume 16. Sage publications, 1996. → pages 73, 74

[221] C. E. Murray, G. E. Horton, C. H. Johnson, L. Notestine, B. Garr, A. M. Pow, P. Flasch, and E. Doom. Domestic violence service providers' perceptions of safety planning: A focus group study. *Journal of Family Violence*, 30(3):381–392, 2015. → page 111

[222] C. E. Murray, A. M. Pow, A. Chow, H. Nemati, and J. White. Domestic violence service providers' needs and perceptions of technology: A qualitative study. *Journal of Technology in Human Services*, 33(2): 133–155, 2015. → page 111

[223] M. Myers. Qualitative research and the generalizability question: Standing firm with proteus. *The qualitative report*, 4(3):9, 2000. → page 97

[224] U. Nations. The impact of digital technologies. https://www.un.org/en/un75/impact-digital-technologies, 2020. Accessed: 2020-09-16. → page 2

[225] Nextiva. Protect your number with call masking. https://www.nextiva.com/features/voip/call-masking.html, 2021. Accessed: 2021-02-24. → page 58

[226] M. Niedźwiedziński and A. Bąkała. Telework and security. *Systems: journal of transdisciplinary systems science*, 12(1), 2007. → page 5

[227] H. Noble and J. Smith. Issues of validity and reliability in qualitative research. *Evidence-based nursing*, 18(2):34–35, 2015. → pages 108, 121

[228] OAuth. The OAuth 2.0 Authorization Framework. https://tools.ietf.org/html/rfc6749, 2019. Accessed: 2019-12-26. → page 22

[229] I. B. of Canada. Cyber risks: An increased threat during covid-19. http://www.ibc.ca/on/business/risk-management/cyber-risk/an-increased-threat-during-covid-19, 2020. Accessed: 2021-01-18. → page 4

[230] H. of Commons. House of commons staff handbook-information security responsibilities. https://www.parliament.uk/documents/commons-resources/Staff-handbook/chapter-23-information-security.pdf, 2017. Accessed: 2019-09-17. → page 4

[231] F. B. of Investigation. National incident-based reporting system. https://www.fbi.gov/services/cjis/ucr/nibrs, 2013. → page 6

[232] U. B. of Labour Statistics. Economic news release. https://www.bls.gov/news.release/flex2.htm, 2020. Accessed: 2020-09-11. → page 4

[233] S. E. of Philosophy. Privacy and information technology. https://plato.stanford.edu/entries/it-privacy/, 2019. Accessed: 2020-09-16. → page 2

[234] K. Okereafor and P. Manny. Solving cybersecurity challenges of telecommuting and video conferencing applications in the covid-19 pandemic. *Journal Homepage: http://ijmr. net. in*, 8(6), 2020. → page 39

[235] M. K. on Sexual Assault. Media kit on sexual assault: Perpetrators. https://www.inspq.qc.ca/en/sexual-assault/understanding/perpetrators, 2020. Accessed: 2019-02-26. → page 79

[236] C. Ontario Ministry of Children and S. Services. Statistics: Sexual violence. http://www.women.gov.on.ca/owd/english/ending-violence/sexual_violence.shtml, 2020. Accessed: 2021-04-15. → pages 6, 87

[237] OpenPGP. Openpgp about. https://www.openpgp.org, 2021. Accessed: 2021-02-1. → page 62

[238] B. Orbach and L. Huang. Con men and their enablers: The anatomy of confidence games. *Social Research: An International Quarterly*, 85(4): 795–822, 2018. → page 115

[239] I. L. Organisation. The gender gap in employment: What's holding women back? https://www.ilo.org/infostories/en-GB/Stories/Employment/barriers-women#intro, 2018. Accessed: 2020-09-11. → page 54

[240] E. Ossiannilsson. The new normal: Post covid-19 is about change and sustainability. *Near East University Online Journal of Education*, 4(1): 72–77, 2021. → page 2

[241] L. Palen and P. Dourish. Unpacking" privacy" for a networked world. In *Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 129–136, 2003. → pages 60, 103

[242] N. Pandey, A. Pal, et al. Impact of digital surge during covid-19 pandemic: A viewpoint on research and practice. *International journal of information management*, 55:102171, 2020. → pages 1, 2

[243] C. J. Pannucci and E. G. Wilkins. Identifying and avoiding bias in research. *Plastic and reconstructive surgery*, 126(2):619, 2010. → pages 108, 121

[244] C. Y. Park, C. Faklaris, S. Zhao, A. Sciuto, L. Dabbish, and J. Hong. Share and share alike? an exploration of secure behaviors in romantic relationships, 2018. → pages 1, 4, 11, 14, 16, 17, 27, 29

[245] S. Parkin, T. Patel, I. Lopez-Neira, and L. Tanczer. Usability analysis of shared device ecosystem security: informing support for survivors of iot-facilitated tech-abuse. In *Proceedings of the New Security Paradigms Workshop*, pages 1–15, 2019. → page 111

[246] U. Parliament. Advice for members and their staff. https://www.parliament.uk/documents/upload/advice-for-members-offices.pdf, 2019. Accessed: 2019-09-17. → page 4

[247] M. A. Pendergrass. *The intersection of human trafficking and technology*. PhD thesis, Utica College, 2018. → page 115

[248] R. Pennington and J. Birthisel. When new media make news: Framing technology and sexual assault in the steubenville rape case. *New Media & Society*, 18(11):2435–2451, 2016. → page 117

[249] S. Perreault. Criminal victimization in canada, 2014. *Juristat*, 35(1):1–43, 2015. → page 6

[250] C. Perricone. The ultimate guide to customer onboarding. https://blog.hubspot.com/service/customer-onboarding#, 2021. Accessed: 2021-06-12. → page 101

[251] A. Perrin and S. Atske. About three-in-ten u.s. adults say they are 'almost constantly' online. https://www.pewresearch.org/fact-tank/2021/03/26/about-three-in-ten-u-s-adults-say-they-are-almost-constantly-online/, 2021. Accessed: 2020-09-16. → page 1

[252] I. Plaisier, A. Beekman, R. De Graaf, J. Smit, R. Van Dyck, and B. Penninx. Work functioning in persons with depressive and anxiety disorders: the role of specific psychopathological characteristics. *Journal of affective disorders*, 125(1-3):198–206, 2010. → page 56

[253] D. F. Polit and B. P. Hungler. *Study Guide for Nursing Research: Principles and Methods*. Lippincott Williams & Wilkins, 1991. → page 97

[254] A. Powell. Configuring consent: Emerging technologies, unauthorized sexual images and sexual assault. *Australian & New Zealand journal of criminology*, 43(1):76–90, 2010. → pages 112, 116, 117

[255] A. Powell. Configuring consent: Emerging technologies, unauthorized sexual images and sexual assault. *Australian & New Zealand journal of criminology*, 43(1):76–90, 2010. → pages 118, 184

[256] A. Powell and N. Henry. *Sexual violence in a digital age*. Springer, 2017. → pages 111, 112, 115, 116, 118

[257] A. Powell and N. Henry. Policing technology-facilitated sexual violence against adult victims: Police and service sector perspectives. *Policing and Society*, 28(3):291–307, 2018. → page 112

[258] A. Powell and N. Henry. Technology-facilitated sexual violence victimization: Results from an online survey of australian adults. *Journal of interpersonal violence*, 34(17):3637–3665, 2019. → page 81

[259] A. Powell and N. Henry. Technology-facilitated sexual violence victimization: Results from an online survey of australian adults. *Journal of interpersonal violence*, 34(17):3637–3665, 2019. → page 117

[260] A. Powell, N. Henry, A. Flynn, and A. J. Scott. Image-based sexual abuse: The extent, nature, and predictors of perpetration in a community sample of australian residents. *Computers in Human Behavior*, 92:393–402, 2019. → page 118

[261] A. Powell, A. Scott, A. Flynn, and N. Henry. Image-based sexual abuse: An international study of victims and perpetrators. *Goldsmiths, University of London*, 2020. → page 117

[262] ProfileLinked. We Create Your Professional Linkedin Profile. https://ca.linkedin.com/company/professional-linkedin-profiles-services-for-executives, 2009. Accessed: 2019-02-28. → page 32

[263] T. Project. About the tor project. https://www.torproject.org, 2021. Accessed: 2021-04-15. → page 114

[264] P. Pyöriä. Knowledge work in distributed environments: issues and illusions. *New Technology, Work and Employment*, 18(3):166–180, 2003. → pages 39, 60

[265] P. Pyöriä. Managing telework: risks, fears and rules. *Management Research Review*, 2011. → page 38

[266] F. G. QC, J. Muraszkiewicz, and N. Vavoula. The role of technology in the fight against human trafficking: Reflections on privacy and data protection concerns. *Computer Law & Security Review*, 32(2):205–217, 2016. → page 111

[267] A. Quan-Haase, A. D. Nevin, and V. Lukacs. Romantic dissolution and facebook life: a typology of coping strategies for breakups. In *Networks, Hacking, and Media–CITA MS@ 30: Now and Then and Tomorrow*, pages 73–98. Emerald Publishing Limited, 2018. → page 14

[268] E. Quayle and M. Taylor. Child seduction and self-representation on the internet. *CyberPsychology & Behavior*, 4(5):597–608, 2001. → pages 114, 115, 116, 117

[269] E. Quayle and M. Taylor. Child pornography and the internet: Perpetuating a cycle of abuse. *Deviant behavior*, 23(4):331–361, 2002. → page 116

[270] A. Queirós, D. Faria, and F. Almeida. Strengths and limitations of qualitative and quantitative research methods. *European Journal of Education Studies*, 2017. → page 40

[271] M. Quiroga. Visible's shift to a permanent work from home model. https://www.linkedin.com/pulse/visibles-shift-permanent-work-from-home-model-miguel-quiroga/?trackingId=28Ku%2F%2Ft4b5g4PVyiJ9PBsA%3D%3D, 2020. Accessed: 2021-01-18. → pages 5, 56, 63

[272] Quora. Is it possible to share access to a LinkedIn profile? https://www.quora.com/Is-it-possible-to-share-access-to-a-LinkedIn-profile, November 2018. Accessed: 2019-02-28. → page 32

[273] S. Raets and J. Janssens. Trafficking and technology: Exploring the role of digital communication technologies in the belgian human trafficking business. *European Journal on Criminal Policy and Research*, pages 1–24, 2019. → page 111

[274] S. Raets and J. Janssens. Trafficking and technology: Exploring the role of digital communication technologies in the belgian human trafficking business. *European Journal on Criminal Policy and Research*, pages 1–24, 2019. → pages 114, 115, 116, 118

[275] F. Raja, K. Hawkey, and K. Beznosov. Revealing hidden context: improving mental models of personal firewall users. In *Proceedings of the 5th Symposium on Usable Privacy and Security*, pages 1–12, 2009. → page 129

[276] N. Ramsay, V. Carr, L. Sailer, M. McDermott, S. Shenai, and D. A. Yassien. Tech vs abuse: Research findings. *Comic Relief*, 2019. → pages 111, 116, 118

[277] Y. Rashidi, K. Vaniea, and L. J. Camp. Understanding saudis' privacy concerns when using whatsapp. In *Proceedings of the Workshop on Usable Security (USEC'16)*, pages 1–8, 2016. → page 60

[278] B. A. Reaves. Felony defendants in large urban counties, 2009-statistical tables. *Washington, DC: US Department of Justice*, 2013. → page 6

[279] Reddit. Black screen or entire screen flickering. https://www.reddit.com/r/Zoom/comments/fyi2ip/black_screen_or_entire_screen_flickering/, 2020. Accessed: 2020-09-17. → page 45

[280] T. Reichherzer, M. Timm, N. Earley, N. Reyes, and V. Kumar. Using machine learning techniques to track individuals & their fitness activities. In *CATA 2017*, pages 119–124. ISCA, 2017. → page 111

[281] E. Research. The smart audio report. https://www.nationalpublicmedia.com/uploads/2020/01/The-Smart-Audio-Report-Winter-2019.pdf, 2019. Accessed: 2021-06-12. → page 99

[282] B. W. Reynolds. Differences between teleworking and telecommuting. https://www.flexjobs.com/blog/post/telecommuting-or-telework-whats-the-difference/, 2020. Accessed: 2020-09-17. → page 38

[283] J. Ross. The business value of user experience. *Cranbury: D3 Infragistics*, 2014. → page 28

[284] R. Ross, M. McEvilley, and J. Oren. Systems security engineering: Considerations for a multidisciplinary approach in the engineering of trustworthy secure systems. Technical report, National Institute of Standards and Technology, 2016. → page 37

[285] C. Rotenberg. From arrest to conviction: Court outcomes of police-reported sexual assaults in canada, 2009 to 2014. *Juristat: Canadian Centre for Justice Statistics*, pages 1–57, 2017. → page 6

[286] C. Rotenberg. Police-reported sexual assaults in canada, 2009 to 2014: A statistical profile. *Juristat: Canadian Centre for Justice Statistics*, 2017. → page 67

[287] E. F. Rothman, D. Exner, and A. L. Baughman. The prevalence of sexual assault against people who identify as gay, lesbian, or bisexual in the united states: A systematic review. *Trauma, Violence, & Abuse*, 12(2):55–66, 2011. → page 67

[288] K. A. Roundy, P. B. Mendelberg, N. Dell, D. McCoy, D. Nissani, T. Ristenpart, and A. Tamersoy. The many kinds of creepware used for interpersonal attacks. In *2020 IEEE Symposium on Security and Privacy (SP)*, pages 626–643. IEEE, 2020. → page 111

[289] M. A. Ruben, M. D. Stosic, J. Correale, and D. Blanch-Hartigan. Is technology enhancing or hindering interpersonal communication? a framework and preliminary results to examine the relationship between technology use and nonverbal decoding skill. *Frontiers in Psychology*, 11: 3800, 2021. → page 1

[290] N. Sambasivan, A. Batool, N. Ahmed, T. Matthews, K. Thomas, L. S. Gaytán-Lugo, D. Nemer, E. Bursztein, E. Churchill, and S. Consolvo. " they don't leave us alone anywhere we go" gender and digital abuse in south asia. In *proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, pages 1–14, 2019. → page 112

[291] SARSAS. Coping with flashbacks. https://www.sarsas.org.uk/grounding/, 2020. Accessed: 2019-02-26. → pages 85, 86, 95

[292] C. Sas and S. Whittaker. Design for forgetting: disposing of digital possessions after a breakup. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 1823–1832. ACM, 2013. → page 15

[293] M. J. Scannell. Online dating and the risk of sexual assault to college students. *Building Healthy Academic Communities Journal*, 3(1):34–43, 2019. → pages 115, 116

[294] K. Schmelz and A. Ziegelmeyer. Reactions to (the absence of) control and workplace arrangements: experimental evidence from the internet and the laboratory. *Experimental economics*, pages 1–28, 2020. → page 5

[295] F. B. Schneider. Least privilege and more [computer security]. *IEEE Security & Privacy*, 1(5):55–59, 2003. → page 33

[296] J. Schofield. How can I protect my data if my laptop is stolen. https://www.theguardian.com/technology/2016/jul/07/how-can-i-protect-my-data-if-my-laptop-is-stolen, 2016. Accessed: 2021-02-1. → page 57

[297] T. Schütz and Z. Stanley-Lockman. Smart logistics for future armed forces. *Cit*, pages 05–11, 2019. → page 1

[298] U. S. Security. Retirement benefits. https://www.ssa.gov/benefits/retirement/planner/agereduction.html, 2020. Accessed: 2020-09-11. → page 54

[299] E. Seto, P. Challa, and P. Ware. Adoption of covid-19 contact tracing apps: A balance between privacy and effectiveness. *Journal of Medical Internet Research*, 23(3), 2021. → page 99

[300] H. Shaikh. The importance of physical security in the workplace. https://resources.infosecinstitute.com/topic/importance-physical-security-workplace/, 2018. Accessed: 2021-02-1. → page 57

[301] R. Shirey. Rfc 4949-internet security glossary, version 2. https://tools.ietf.org/html/rfc4949, 2007. Accessed: 2021-02-24. → page 37

[302] S. Singh, A. Cabraal, C. Demosthenous, G. Astbrink, and M. Furlong. Password sharing: implications for security design based on social practice, 2007. → pages 1, 13

[303] Skype. How do i customize my background for skype video calls? https://support.skype.com/en/faq/fa34896/how-do-i-customize-my-background-for-skype-video-calls, 2021. Accessed: 2021-02-19. → page 45

[304] E. B. Slotter, W. L. Gardner, and E. J. Finkel. Who am i without you? the influence of romantic breakup on the self-concept. *Personality and Social Psychology Bulletin*, 36(2):147–160, 2010. → page 27

[305] A. Smith. Record shares of americans now own smartphones, have home broadband. https://www.pewresearch.org/fact-tank/2017/01/12/evolution-of-technology/, 2021. Accessed: 2020-09-16. → page 1

[306] S. G. Smith, X. Zhang, K. C. Basile, M. T. Merrick, J. Wang, M.-j. Kresnow, and J. Chen. *The national intimate partner and sexual violence survey: 2015 data brief–updated release*. National Center for Injury Prevention and Control, Centers for Disease Control and Prevention, 2018. → pages 6, 87

[307] C. Snook. Safelives. *Tech vs abuse: research findings*, 2017. → pages 110, 111

[308] C. Southworth, S. Dawson, C. Fraser, and S. Tucker. A high-tech twist on abuse: Technology, intimate partner stalking, and advocacy. *Violence Against Women Online Resources*, 2005. → page 111

[309] D. Spinellis, S. Kokolakis, and S. Gritzalis. Security requirements, risks and recommendations for small enterprise and home-office environments. *Information Management & Computer Security*, 1999. → pages 39, 61

[310] Statista. Number of social network users worldwide from 2017 to 2025(in billions). https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/, 2021. Accessed: 2020-09-16. → page 1

[311] K. E. Stonard, E. Bowen, T. R. Lawrence, and S. A. Price. The relevance of technology to the nature, prevalence and impact of adolescent dating violence and abuse: A research synthesis. *Aggression and violent behavior*, 19(4):390–417, 2014. → pages 111, 112, 113, 117

[312] A. Sturgeon. Telework: threats, risks and solutions. *Information Management & Computer Security*, 1996. → page 39

[313] D. Sward. User experience design: a strategy for competitive advantage. *AMCIS 2007 Proceedings*, page 163, 2007. → page 28

[314] L. Tanczer, I. Neria, S. Parkin, T. Patel, and G. Danezis. Gender and iot research report. the rise of the internet of things and implications for technology-facilitated abuse, 2018. → pages 111, 119, 183

[315] L. Tanczer, S. Parkin, T. Patel, I. Lopez-Neira, and J. Slupska. Ucl's gender and internet of things (iot) research project, 2019. → page 111

[316] Taster. Google scholar, web of science, and scopus: Which is best for me?, 2019. URL https://blogs.lse.ac.uk/impactofsocialsciences/2019/12/03/google-scholar-web-of-science-and-scopus-which-is-best-for-me/. → pages 108, 121

[317] M. C. Taylor. *Confidence games: Money and markets in a world without redemption*. University of Chicago Press, 2004. → page 115

[318] M. Teams. Change your background for a teams meeting. https://support.microsoft.com/en-us/office/change-your-background-for-a-teams-meeting-f77a2381-443a-499d-825e-509a140f4780, 2021. Accessed: 2021-02-19. → page 45

[319] M. Teams. How to live stream microsoft teams meeting to youtube, facebook live & others. https://www.youtube.com/watch?v=fGMYvHrIB6M, 2021. Accessed: 2021-02-1. → page 60

[320] M. Teams. User presence in teams. https://docs.microsoft.com/en-us/microsoftteams/presence-admins, 2021. Accessed: 2021-02-1. → page 47

[321] B. S. Trask. Personal relationship, 2011. → page 2

[322] E. Tseng, R. Bellini, N. McDonald, M. Danos, R. Greenstadt, D. McCoy, N. Dell, and T. Ristenpart. The tools and tactics used in intimate partner surveillance: An analysis of online infidelity forums. In *29th {USENIX} Security Symposium ({USENIX} Security 20)*, pages 1893–1909, 2020. → page 111

[323] Z. Tufekci. Can you see me now? audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology & Society*, 28 (1):20–36, 2008. → pages 60, 103

[324] D. Turner. Should you use inter-rater reliability in qualitative coding?, March 12, 2020. URL https://www.quirkos.com/blog/post/inter-rater-reliaiblity-qualitative-coding-data/. → page 109

[325] Twitter. How to use the teams feature on tweetdeck. https://help.twitter.com/en/using-twitter/tweetdeck-teams, 2019. Accessed: 2019-09-18. → page 33

[326] C. Underhill and M. G. Olmsted. An experimental comparison of computer-mediated and face-to-face focus groups. *Social Science Computer Review*, 21(4):506–512, 2003. → page 77

[327] C. M. University. Iot security & privacy label. https://www.iotsecurityprivacy.org, 2021. Accessed: 2021-04-14. → page 130

[328] L. Uusitalo et al. Designing for women experiencing intimate partner violence. Master's thesis, Aalto University, 2018. → page 100

[329] UXPlanet. Why better web user experience leads to better branding. https://uxplanet.org/why-better-web-user-experience-leads-to-better-branding-e2194ff0d081, 2019. Accessed: 2019-09-18. → page 28

[330] A. van Moorsel, M. Emms, G. Rendall, and B. Arief. Digital strategy for the social inclusion of survivors of domestic violence. *Technical report. CS-TR-1277*, 2011. → pages 111, 116

[331] P. C. van Oorschot. *Computer Security and the Internet*. Springer, 2020. → pages 37, 100, 103

[332] VeraCrypt. Veracrypt about. https://www.veracrypt.fr/en/Home.html, 2021. Accessed: 2021-02-1. → page 57

[333] VESTA. Vesta social innovation technologies. https://www.vestasit.com, 2020. Accessed: 2021-04-14. → pages vii, 70

[334] A. Vinciarelli. Body language without a body: nonverbal communication in technology mediated settings. In *Proceedings of the 1st ACM SIGCHI International Workshop on Investigating Social Interactions with Artificial Agents*, pages 2–3, 2017. → page 1

[335] J. Vitak, C. Lampe, R. Gray, and N. B. Ellison. "why won't you be my facebook friend?" strategies for managing context collapse in the workplace. In *Proceedings of the 2012 iConference*, pages 555–557, 2012. → page 60

[336] L. Vitis, M. A. Joseph, and M. D. Mahadevan. Technology and sexual violence: Sacc summary report. *Sexual Assault Care Centre*, 2017. → pages 112, 114, 115, 116, 117, 118, 119

[337] E. Vogels. Millennials stand out for their technology use, but older generations also embrace digital life. https://www.pewresearch.org/fact-tank/2019/09/09/us-generations-technology-use/, 2021. Accessed: 2020-09-16. → page 1

[338] L. Von Ahn, M. Blum, N. J. Hopper, and J. Langford. CAPTCHA: Using hard AI problems for security. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 294–311. Springer, 2003. → page 93

[339] D. Voth. Using ai to detect breast cancer. *IEEE Intelligent Systems*, 20(1): 5–7, 2005. → page 1

[340] J. Webb. Anonymity vs privacy vs security understanding the shades of safety online. https://highspeedexperts.com/online-security-privacy/anonymity-vs-privacy-vs-security/, 2020. Accessed: 2019-02-26. → pages 88, 101

[341] M. Webster. Sexual assault. https://www.merriam-webster.com/dictionary/rape, 2021. Accessed: 2021-04-12. → page 106

[342] N. Westmarland, M. Hardey, H. Bows, D. Branley, M. Chowdhury, K. Wheatley, and R. Wistow. Protecting women's safety? the use of smartphone 'apps' in relation to domestic and sexual violence. *Society for Applied Social Sciences*, 2013. → pages 110, 111, 112, 116

[343] N. Whaley. Surveillance in employment: The case of teleworking. *Technical Communication*, 47(2):260–260, 2000. → page 38

[344] A. Whitten and J. D. Tygar. Why johnny can't encrypt: A usability evaluation of pgp 5.0. In *USENIX Security Symposium*, volume 348, pages 169–184, 1999. → page 62

[345] M. Whitty, J. Doodson, S. Creese, and D. Hodges. Individual differences in cyber security behaviors: an examination of who is sharing passwords. *Cyberpsychology, Behavior, and Social Networking*, 18(1):3–7, 2015. → pages 21, 27

[346] WHO. Who reports fivefold increase in cyber attacks, urges vigilance. https://www.who.int/news-room/detail/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance, 2020. Accessed: 2020-09-11. → pages 5, 63

[347] P. Wijesekera, A. Baokar, L. Tsai, J. Reardon, S. Egelman, D. Wagner, and K. Beznosov. The feasibility of dynamically granted permissions: Aligning mobile privacy with user preferences. In *2017 IEEE Symposium on Security and Privacy (SP)*, pages 1077–1093. IEEE, 2017. → page 104

[348] P. Wijesekera, J. Reardon, I. Reyes, L. Tsai, J.-W. Chen, N. Good, D. Wagner, K. Beznosov, and S. Egelman. Contextualizing privacy decisions for better prediction (and protection). In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, pages 1–13, 2018. → page 104

[349] P. Willis. Learning to labour (London, Saxon House). *WillisLearning to Labour1977*, 1977. → page 73

[350] J. F. Wolfswinkel, E. Furtmueller, and C. P. Wilderom. Using grounded theory as a method for rigorously reviewing literature. *European journal of information systems*, 22(1):45–55, 2013. → pages 107, 109

[351] M. Wong. Stanford research provides a snapshot of a new working-from-home economy. https://news.stanford.edu/2020/06/29/snapshot-new-working-home-economy/, 2020. Accessed: 2020-09-11. → page 4

[352] D. Woodlock. The abuse of technology in domestic violence and stalking. *Violence against women*, 23(5):584–602, 2017. → pages 111, 112, 113

[353] J. Xu, K. Le, A. Deitermann, and E. Montague. How different types of users develop trust in technology: A qualitative analysis of the antecedents of active and passive user trust in a shared technology. *Applied ergonomics*, 45(6):1495–1503, 2014. → page 72

[354] K.-P. Yee. User interaction design for secure systems. In *International Conference on Information and Communications Security*, pages 278–290. Springer, 2002. → page 31

[355] K.-P. Yee. User interaction design for secure systems. In *International Conference on Information and Communications Security*, pages 278–290. Springer, 2002. → page 62

[356] K. Yoshigoe, W. Dai, M. Abramson, and A. Jacobs. Overcoming invasion of privacy in smart home environment with synthetic packet injection. In *2015 TRON Symposium (TRONSHOW)*, pages 1–7. IEEE, 2015. → page 111

[357] Y. Zhang, F. Monrose, and M. K. Reiter. The security of modern password expiration: An algorithmic framework and empirical analysis. In *Proceedings of the 17th ACM conference on Computer and communications security*, pages 176–186. ACM, 2010. → page 22

[358] D. Zinoviev and V. Duong. Toward understanding friendship in online social networks. *arXiv preprint arXiv:0902.4658*, 2009. → page 114

[359] Zoom. Virtual background. https://support.zoom.us/hc/en-us/articles/210707503-Virtual-background, 2020. Accessed: 2020-09-17. → page 45

[360] Zoom. Live streaming meetings or webinars using a custom service. https://support.zoom.us/hc/en-us/articles/115001777826-Live-Streaming-Meetings-or-Webinars-Using-a-Custom-Service, 2021. Accessed: 2021-02-1. → page 60

Appendix A

Challenges in Online Reporting of Sexual Assault

A.1 Questions from the P-TPRS shown to Participants from Page 2 and 3

1. Date of Assault
2. Time of Assault
3. Location of Assault
4. Description of Complainant:
    - Male
    - Female
5. Age
6. Height
7. Weight
8. Build
9. Hair Colour

10. Style

11. Length

(A) Offender's Name: (if known)

(B) Offender's Address:

(C) Description of Offender :

- Male
- Female
- Colour
- Race
- Age
- Height
- Weight
- Build
- Hair Colour
- Style
- Length
- Facial Features
- Facial Hair
- Complexion
- Eye Colour
- Glasses
- Circumcised
- Scars/Tattoos/Birthmarks Etc.
- Clothing Worn at Time of Sexual Assault

- Distinguishing Characteristics

(a) Vehicle Information (Licence #, Make, Model, Colour, Damage, Anything Distinguishable)

(b) Details of Offense: (EXPLAIN IN COMPLAINANT'S OWN WORDS)

A.2 Sample of the O-TPRS Prototype Shown to Participants

Figure A.1: O-TPRS homepage

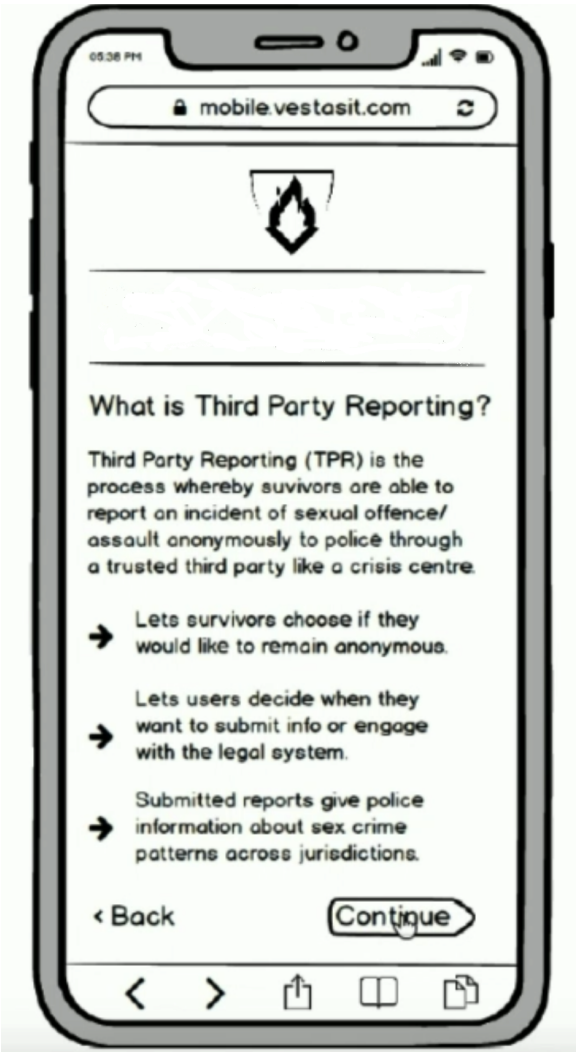

Figure A.2: Introduction to TPRS

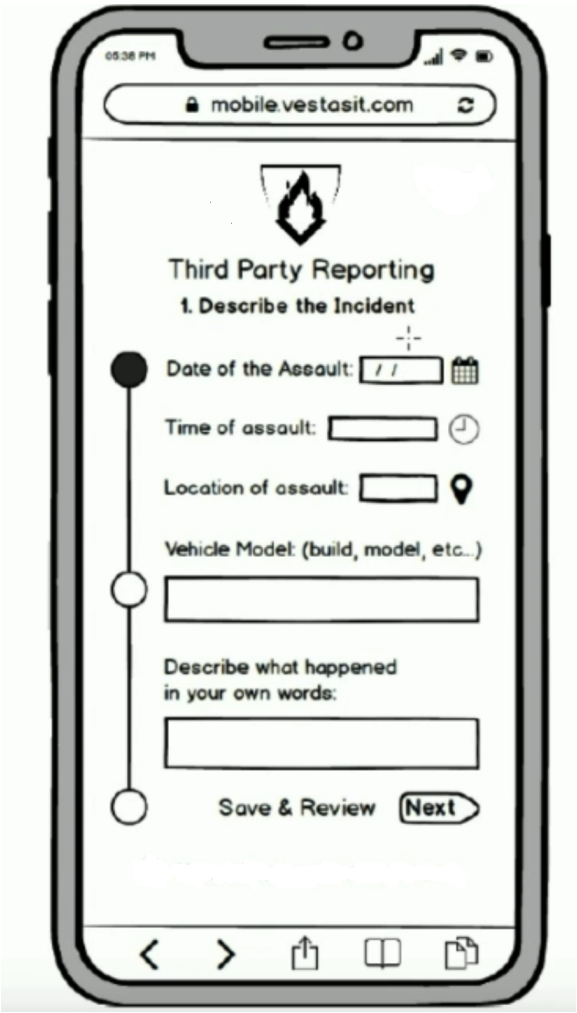

Figure A.3: O-TPR form page 1

Figure A.4: O-TPR form page 2

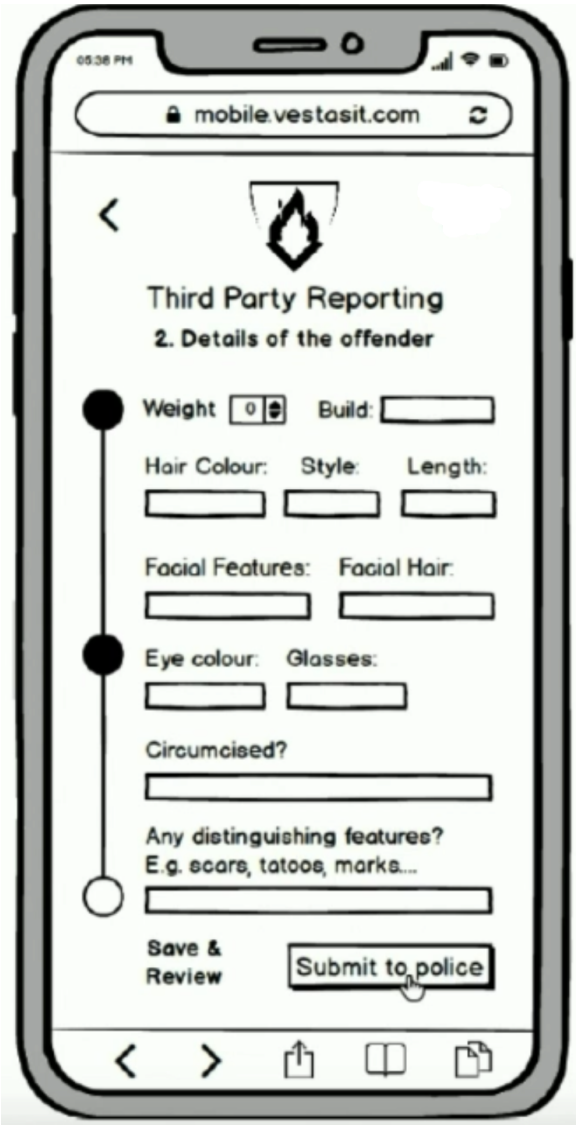

Figure A.5: O-TPR form page 3

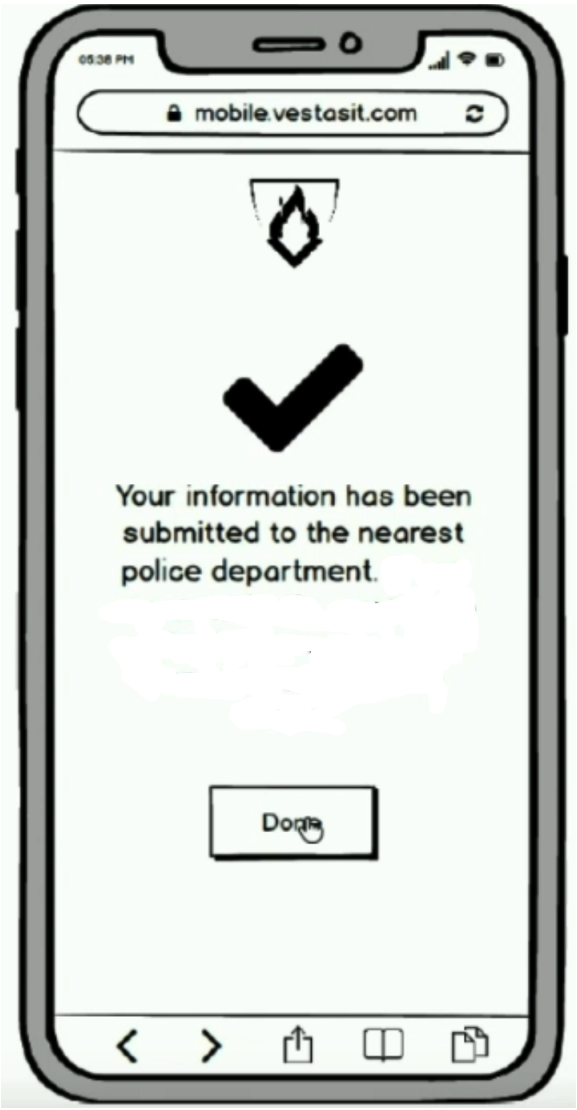

Figure A.6: Submission page

Appendix B

Challenges and Threats of Mass Telecommuting

B.1 Interview Guide

Demographic questions

1. Age
2. Gender
3. Educational level
4. Place of work
5. Position at work

Interview questions

1. How has the pandemic affected your life?
2. How has it changed your life?
3. How has it changed your life in relation to others living with you?
4. Describe your typical work day before the pandemic

5. How many hours do you work?
6. Did you work remotely from home before the pandemic? If yes, how frequently?
7. How long have you been working from home?
8. If yes to the above question, how does your current remote work differ from previous experiences?
9. What is your experience working from home?
10. Describe your day-to-day work activities from home?
11. How does your current work activities differ from working in your physical office space?
12. What technology (or software, machines, devices) did you use to work with in the physical office space?
13. How do you handle/work with confidential communications in your work environment?
14. How do you manage confidential documents in your work environment?
15. What, if anything, is your workplace's guide on handling confidential communications and documents from home?
16. What, if anything, are the measures taken to comply with the organization's work-at-home rules?
17. What makes it easy to comply with these rules?
18. What makes it difficult to comply with these rules?
19. What motivates you, if anything, to be secured when you work from home?
20. What are your concerns, if any, with working from home as opposed to working in the office?

21. List the new technologies or software used specifically to work from home
22. What software or technologies have you explored since working from home?
23. If not mentioned ask, what video conferencing softwares have you been using to work from home?
24. If not mentioned ask, do you use VPNs to access your organization's resources?

    For each technology used for remote working, ask:

25. Why did you choose this technology?
26. What if anything makes it easy to use the software? Why?
27. What if anything makes it difficult/complex to use the software?
28. If any complexity is discussed: How do you mitigate the complexities of using these technologies?
29. How does the technology assist you in securing your organization's confidential documents and communications?
30. How does the technology assist you in complying with your company's guide on protecting confidential documents and communications?
31. If you could change how the technology currently works, what would you change and why?
32. How do you handle concerns related to people in the household?
33. How is your current work environment?
34. What, if anything, would you like to change about your current work environment?
35. What other information do you think will be useful for this research?

Appendix C

Characteristics of Technology

C.1 Code Book

Theme	Sub-themes	Definitions	Examples
1. How technology facilitates sexual assault	The anonymity nature of technology	Perpetrators hide under the cover of 'anonymity' and use technology for purposes other than intended	"Recent technological advances also enable offenders to disguise their identities and prevent the source of their communications from being discovered by law enforcement. The use of cryptography, stenography and anonymising protocols make the task of tracking communications difficult for police and regulators alike" [56].
	The malleability nature of technology	The use of technology to suit whatever perpetrators want it to be	"Technologies developed to detect surveillance ... may have the potential to be abused by those attempting to evade surveillance by law enforcement, much in the same way that many existing privacy and security technologies can be abused by criminals to hinder investigations." [**?**].
	Lack of well-defined boundaries	No physical limit to the perpetrator's reach	"Participants felt that the fluidity between online and offline social spheres was a core feature of young people's lives. Specifically, participants identified: — the centrality of online sociality to young people's interactions; — the blurring between online and offline domains " [26].

	Networking	Perpetrators using technology to network with other perpetrators and form stronger bond	“The Internet may make it easier for CSEC (Cybersecurity) offenders to make connections with other offenders, for example, networking among pimps.” [217].
	Monitoring victims	The use of technology to monitor the activities of victims	“Computer monitoring software can track and record every keystroke a person makes on a computer. Location tracking devices, such as GPS, can track victims’ daily movements and their real-time location. Hidden cameras and audio bugs have become much smaller and more affordable so it is easier ... to install surveillance devices inside a victim’s home, car, or workplace” [107].
	The friendship nature of technology	The use of technology to facilitate friendship between the perpetrator and the potential victim	“After a potential victim has been identified, the offender will attempt to initiate a conversation or relationship through email, chat, Instant Messaging (IM) or friend requests on social networking sites. The friendship and relationship forming stages are similar to those of the development of other online friendships, and involve the offender approaching and be friending the young person, and encouraging them to discuss their life in order to initiate friendship” [36].
	Technology is opaque and a blackbox	Technology is not transparent	“The blackbox nature of technology was seen as a problematic factor. Participants were concerned with their own lack of knowledge regarding the data that their own devices collect and with whom this data may be shared” [314].
	Forgery of identity	Perpetrators changing their identity using technology	“This case identifies an additional method of facilitation afforded by new technologies, namely the ability of the perpetrator to create a false representation of themselves to deceive potential victims. The advantage for offenders of this behaviour is that initial and continued engagement is more likely in circumstances where the perpetrator is able to misrepresent themselves as a desirable entity.” [26].

	Technology is ever-changing	Perpetrators using the evolving nature of technology against victims	"Offenders can use technology to adapt their offending behaviour. Consequentially, the constant and continual evolution in technology has ramifications with regard to the facilitation and of child sexual abuse and the impact that they have on the prevention of child sexual abuse" [204].
	Distribution of unauthorised materials	The use of technology for the distribution of unauthorized sexual images where a sexual assault has occurred	"In particular, rather than viewing the use of emerging ICTs (Information and Communications Technology) as representing an extension on video voyeurism or indeed as a driver of sexual violence, it is argued that this issue must be considered in light of a continuum of sexual violence. This is not to undermine the importance of securing justice and support for victims regarding the original sexual assault, but rather emphasises the continued assault on the victim where an image is recorded and distributed." [255].
	Publicly available information through technology	The use of technology to view and gather publicly available information that is used against victims	"In addition to using technology to monitor and track victims ... using the Internet to gather information about their victims, post damaging information about victims, and even impersonate victims" [107].
	The reproducibility or irreversibility of technology	The reproducibility of technology aiding sexual abuse	"Two of the affordances that social media platforms such as Twitter offer are (a) the ability to share content in live time and (b) the ability to screenshot and capture content that then remains as a digital image, even after the original content is deleted" [95].
	Initiating meeting between the perpetrator and the victim	The use of technology to initiate meeting between the victim and the perpetrator	"The use of social networking sites to invite women to meet in the physical domain—police have described how sites may be flooded with invitations from an individual, increasing their chances of a meeting, then the woman is sexually assaulted, and multiple perpetrators may be involved" [26].

	Accessibility and indispensability of technology	Technology is easily accessible and indispensable making it easy to misuse	“ " How technology is used in intimate terrorism-Social Media is now a ubiquitous technology that connects people virtual.” [88].
	Legitimate tools can be misused	Technology allows legitimate tools to be used in illegitimate ways	“Our data also revealed how abusers often leverage what we term dual-use applications to spy on victims. Unlike software that is clearly designed and marketed to be spyware, dual-use applications are designed for legitimate purposes, such as anti- theft tracking apps, ‘Find My Friends’emergency response apps, parental control apps, and other” [110].

Table C.1: The tables shows various sub-themes that emerged during our coding process. We grouped and renamed similar sub-themes. The grouped themes are presented in the Results sections. An overarching theme around this set of sub-themes is ‘How Technology Enables Abuse’. Each sub-themes reflected this theme—this theme became the main theme around this set of sub-themes.