


# Towards Understanding Privacy and Trust in Online Reporting of Sexual Assault

Borke Obada-Obieh, *University of British Columbia;* Lucrezia Spagnolo, *Vesta Social Innovation Technologies;* Konstantin Beznosov, *University of British Columbia*

https://www.usenix.org/conference/soups2020/presentation/obada-obieh

This paper is included in the Proceedings of the Sixteenth Symposium on Usable Privacy and Security.

August 10–11, 2020

978-1-939133-16-8

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

# Towards Understanding Privacy and Trust in Online Reporting of Sexual Assault

Borke Obada-Obieh
*University of British Columbia*
*borke@ece.ubc.ca*

Lucrezia Spagnolo
*Vesta Social Innovation Technologies*
*lucrezia@vestasit.com*

Konstantin Beznosov
*University of British Columbia*
*beznosov@ece.ubc.ca*

## Abstract

According to the United States Department of Justice, every 73 seconds, an American is sexually assaulted. However, sexual assault is under-reported. Globally, 95% of sexual assault cases are unreported, and at most, 5 out of every 1,000 perpetrators end up in prison. Online anonymous third-party reporting systems (O-TPRSs) are being developed to encourage reporting of sexual assaults and to apprehend serial offenders. This paper reports survivors' concerns with trusting and using an O-TPRS. We conducted focus groups and interviews with 35 participants who are sexual assault survivors, support workers, or both. We asked questions related to participants' concerns with trusting an O-TPRS. Our results suggest that participants had technological and emotional concerns that are related to survivors' security and privacy. We provide insights into the challenges of designing O-TPRSs to increase the reporting of sexual assault.

## 1 Introduction

The goal of our research 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 anonymous third-party reporting (TPR) is a response to the clear need for a confidential and accessible platform that survivors of sexual assault can use to communicate their experiences in the hope of holding perpetrators accountable.

Copyright is held by the author/owner. Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee.
*USENIX Symposium on Usable Privacy and Security (SOUPS)* 2020.
August 9–11, 2020, Virtual Conference.

The stark reality is that 1 in 3 Canadian women will experience sexual assault in their adult life [50]. Further, 1 in 14 American men and 1 in 5 American women have been victims of completed or attempted sexual assault during their lifetime [60]. 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 [14, 19]. One in four survivors reported that they had difficulty carrying out everyday activities because of the incident [43]. 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 [20, 42, 43].

However, statistics alone fail to capture the significant repercussions of sexual assault on survivors, not only because the effects of such trauma are unquantifiable [14] but also because sexual assault is greatly underreported [48, 55]. Only 5% of cases are reported to the police [51], and only 11% of those reported cases eventually lead to the conviction of the perpetrator [56]. The reluctance of survivors to report the crime to the police has mainly been attributed to the cumbersome reporting process and to the grueling interview procedure involved in filing a formal police report, which can be adversarial and emotionally very unpleasant for survivors [39, 43, 44, 53, 54].

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 [11], who remains anonymous. Third-party reporting systems (TPRSs) allow survivors to anonymously report sexual assault to the police through a community-based support center [11, 40]. 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 [40]. 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 [11]. 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 [10]. The resulting filing of formal police reports has led to an increase in arrests of serial offenders [10].

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) [11, 40]. Further, third-party reporting is also not available in all sexual assault support centers but only in a few select jurisdictions [11, 13], which defeats its purpose of increasing sexual assault reporting [40, 57]. 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 [7, 9, 20, 42, 58]. Some research also investigates the reporting experiences of survivors [7], including sexual assaults within the armed forces [17] and police-reported sexual assaults against youths and children [18]. 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:

1. RQ1: What are survivors' privacy and security concerns (if any) regarding trusting O-TPRSs?
2. RQ2: 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 [31]." The act of measuring trust is used to predict whether survivors would make use of O-TPRS technology [32]. 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.

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

Our study has two major contributions. First, 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 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*. Second, 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. 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. We are optimistic that when O-TPRSs are designed with careful attention to users' feedback and research, such systems could increase reporting.

## 2 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.

### 2.1 P-TPRS

#### 2.1.1 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 C for the questions asked on a sample P-TPR form.)

#### 2.1.2 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 [11].

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 [11]. Figure 1 shows the P-TPR process.

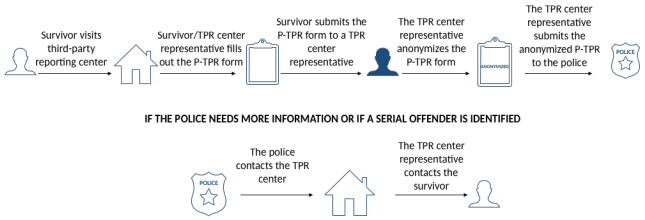



Figure 1: P-TPR process

## 2.2 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.

### 2.2.1 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) [62]. The O-TPRS includes a cover page and pages to type out information about the survivor, offender, and the offense (see Appendix D for a sample of an O-TPRS prototype).

### 2.2.2 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 2 shows the O-TPRS process.

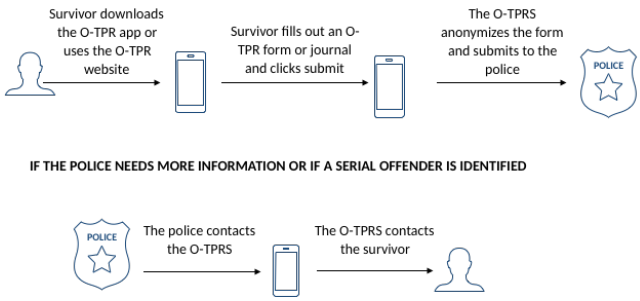



Figure 2: O-TPR process

## 2.3 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 [45]." Prior work shows that heightened levels of trust are associated with heightened levels of intended use [27]. Trust in technology is used to predict the intended or actual adoption of technology [66]. It is also connected to appropriate and inappropriate use of technology [46] and technology over- and under-reliance [5].

Many works on technology and trust exist. Hardre, for instance, studied when, how, and why people trust technology too much [31]. 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 [31].

Minimal research has been done on how survivors build trust in sexual assault technology. Work by Liu is closest to ours [41]. 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 [41] 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.

## 3 Methodology

### 3.1 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 D 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 [47, 65]. As suggested by Hammarberg et al. [30] and illustrated by Willis [65], 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 [47]. 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 [16]. We also offered focus groups because focus groups allow participants to discuss sensitive or controversial topics in a group setting [47]. Due to participants' shared experience, sometimes focus groups "reveal aspects of experiences and perspectives that would not be as accessible without group interaction [47]," which leads to a better quality of data on sensitive topics [47].

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. Appendix A shows participants who self-identified as survivors.

### 3.2 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 2.1, 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 2.2 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 [23]. Further, online focus groups have been found to be useful for reaching members of hard-to-reach populations [24]. Underhill and Olmsted [61] 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.

### 3.3 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 [29], a "set of procedures designed to identify and examine themes from textual data in a way that is transparent and credible [28]." We followed the data analysis steps outlined by Guest et al. [28].

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. Appendix B shows the saturation graph depicting the total number of codes after each interview.

### 3.4 Participants

We recruited 35 participants (33 women and 2 men), aged 19 to 80 years (the mean age was 40 and median was 36). Appendix A 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 Results

To better understand survivors' concerns regarding trusting an O-TPRS, we grouped our findings into **technological** and **emotional** concerns. We define *technological* 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 paper, we use SW, SR, and SWSR along with participants' ID to indicate if participants are support workers, survivors, or both respectively.

## 4.1 Technological Concerns

### 4.1.1 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 to a human versus online, 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 [3] 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** [49] 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."*

### 4.1.2 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."*

### 4.1.3 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 2.1 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."*

### 4.1.4 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.**

#### 4.1.5 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 [33–36, 52].

#### 4.1.6 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 [41] 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.

#### 4.1.7 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.

#### 4.1.8 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."*

#### 4.1.9 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]."*

#### 4.1.10 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 2.2 on how O-TPRS works). However, this format 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 [59] 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]."*

### 4.2 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.

#### 4.2.1 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 [59] 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."*

#### 4.2.2 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."*

## 5 Discussion

### 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 [50, 60]. 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 [21].

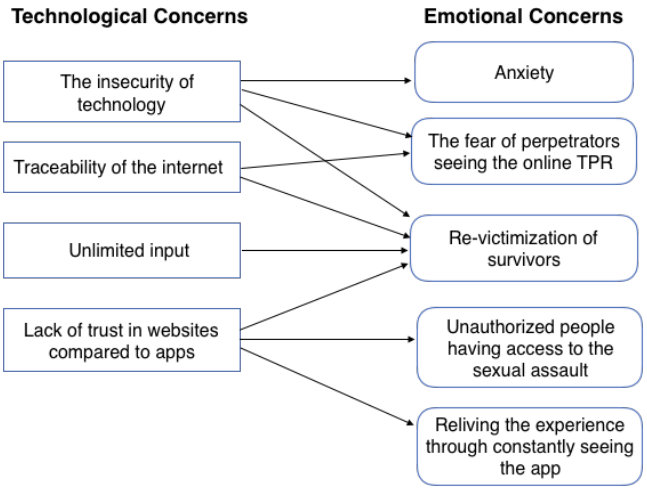



Figure 3: The relationship between technological and emotional concerns

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.

### 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 [64] 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 *actions* of a user in the O-TPRS system but *not* user's *identity*. Table 1 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 1: 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 4.1.1, 4.1.4, 4.1.7, and 4.1.8.)

**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 4.1.3.)

**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 4.1.1, 4.1.2, 4.1.7, and 4.1.8.)

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 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 4.1.1 and 4.1.4). 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 4.2.2). 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.

## 5.3 Trust of survivors in an O-TPRS

### 5.3.1 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. [4] 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. [25] 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 4.1.7 and P22-SWSR in Section 4.1.4), 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 4.1.7). 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 4.1.4). If the perpetrator see this information, it could cause re-victimization of the survivor. For survivors of domestic violence, Arief et al. [4] 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 [15], or they could also make use of a Tor browser [8]. 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 4.1.2). 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 [38], and as cited by P18-SWSR in Section 4.1.5, 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.

#### 5.3.2 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 4.1.1). Further, unauthorized individuals should be unable to discover that the survivor sent the information to the police (for instance, see Section 4.1.4). 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 [26]. It is also difficult to measure how much security is good enough to protect a system. As argued by Hurlburt [37], security may never be good enough. The author explain further that for a secure system to be impenetrable by anyone, the system can probably not be connected to the internet, and humans will have to be taken out of the loop [37]. 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 4.1.1, 4.1.7). The O-TPRS operator will also have to convince survivors that such measures are good enough to protect their information.

### 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 4.1.6, 4.2.2). 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 2 and Table 1). 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 2.1). The police may trust that the report is valid because they trust the representative [12, 45].

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) [63]. 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 2, 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 [22].

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 re-

porting. In addition, as explained by P1-SW in Section 4.1.6, 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 [6]. 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 2, that follow-up would simply be an invitation to make a formal report, which the survivor was free to do at any time anyway.

## 5.5 The provision of human support

The importance of human support when reporting a sexual assault was discussed by many participants (see Sections 4.2.1 and 4.2.2). 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 [59]. For instance, sometimes survivors deal with flashbacks or disassociation from the present moment and need support before, during, and after making a report [59].

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 4.2.1). This design also doesn't address the problem of verifying that the survivor is ready to make a report [59]. 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 4.1.10). Further research is necessary to identify unique solutions to ensure that the survivor is ready, before submitting a report to the O-TPRS.

## 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 4.1.10). 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.

# 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 consideration 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.

# 7 Acknowledgements

This research has been supported by the funding from Vesta Social Innovation Technologies Inc. and Mitacs Accelerate program. We thank members of the sexual assaults centers and all participants who were involved in the study. We thank members of the UBC Laboratory for Education and Research in Secure Systems Engineering (LERSSE) who provided their feedback on the reported research and the earlier versions of the paper. We thank our anonymous reviewers for all the feedback and suggestions they provided for improving the paper. Stylistic and copy editing by Eva van Emden helped to improve readability of this paper.

## References


[1] Ruba Abu-Salma and Benjamin 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.

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

[3] Ildemaro Araujo and Iván 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.

[4] Budi Arief, Kovila PL Coopamootoo, Martin Emms, and Aad 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.

[5] J Elin Bahner, Anke-Dorothea Hüper, and Dietrich 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.

[6] Laura-Kate Bernstein. Investigating and prosecuting swatting crimes. *US Att'ys Bull.*, 64:51, 2016.

[7] Shannon Brennan and Andrea Taylor-Butts. *Sexual assault in Canada, 2004 and 2007*. Canadian Centre for Justice Statistics Ottawa, Ontario: Statistics Canada, 2008.

[8] Tor Browser. Defend yourself. protect yourself against tracking, surveillance, and censorship. https://www.torproject.org/download/, 2020. Accessed: 2019-02-27.

[9] Clayton M Bullock and Mace 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.

[10] British Columbia 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.

[11] British Columbia 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.

[12] Lemuria Carter and France Bélanger. The utilization of e-government services: Citizen trust, innovation and acceptance factors. *Information systems journal*, 15(1):5–25, 2005.

[13] 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.

[14] Yingyu Chen and Sarah 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.

[15] Google Chrome. Browse in private. https://support.google.com/chrome/answer/95464?co=GENIE.Platform%3DDesktop&hl=en, 2020. Accessed: 2019-02-27.

[16] Deborah Cohen and Benjamin Crabtree. Qualitative research guidelines project. http://www.qualres.org/, 2006.

[17] Adam Cotter. *Sexual misconduct in the Canadian Armed Forces, 2016*. Statistics Canada, 2016.

[18] Adam Cotter and Pascale Beaupré. Police-reported sexual offences against children and youth in canada, 2012. *Juristat: Canadian Centre for Justice Statistics*, page 1, 2014.

[19] Danielle Couch, Pranee Liamputtong, and Marian 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.

[20] Beata Cybulska. Sexual assault: Key issues. *Journal of the Royal Society of Medicine*, 100(7):321–324, 2007.

[21] Diane Dodd-McCue and Alexander Tartaglia. Self-report response bias: Learning how to live with its diagnosis in chaplaincy research. *Chaplaincy Today*, 26(1):2–8, 2010.

[22] John R Douceur. The Sybil attack. In *International workshop on peer-to-peer systems*, pages 251–260. Springer, 2002.

[23] Sarah M Flanagan, Sheila Greenfield, Jane Coad, and Susan Neilson. An exploration of the data collection methods utilised with children, teenagers and young people (ctyps). *BMC research notes*, 8(1):61, 2015.

[24] Sarah G Forrestal, Angela Valdovinos D'Angelo, Lisa Klein Vogel, et al. Considerations for and lessons learned from online, synchronous focus groups. *Survey Practice*, 8(2):1–8, 2015.

[25] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. "A stalker's paradise" How intimate partner abusers exploit technology. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, pages 1–13, 2018.

[26] Michael P Gallaher, Brent R Rowe, Alex V Rogozhin, and Albert N Link. Economic analysis of cyber security. Technical report, Research Triangle Inst (RTI) Research Triangle Park NC, 2006.

[27] David Gefen, Elena Karahanna, and Detmar W Straub. Trust and TAM in online shopping: An integrated model. *MIS quarterly*, 27(1):51–90, 2003.

[28] Gregory Guest, Kathleen M MacQueen, and Emily E Namey. *Applied thematic analysis*. Sage Publications, 2011.

[29] Gregory Guest, Kathleen M MacQueen, and Emily E Namey. Introduction to applied thematic analysis. *Applied thematic analysis*, 3:20, 2012.

[30] Karin Hammarberg, Maggie Kirkman, and Sheryl de Lacey. Qualitative research methods: When to use them and how to judge them. *Human reproduction*, 31(3):498–501, 2016.

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

[32] Gert Helgesson, Mats G Hansson, Johnny Ludvigsson, and Ulrica Swartling. Practical matters, rather than lack of trust, motivate non-participation in a long-term cohort trial. *Pediatric diabetes*, 10(6):408–412, 2009.

[33] Nicola Henry and Anastasia Powell. The dark side of the virtual world. In *Preventing Sexual Violence*, pages 84–104. Springer, 2014.

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

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

[36] Nicola Henry and Anastasia Powell. Sexual violence in the digital age: The scope and limits of criminal law. *Social & Legal Studies*, 25(4):397–418, 2016.

[37] George Hurlburt. "Good enough" security: The best we'll ever have. *Computer*, 49(7):98–101, 2016.

[38] Eric Jardine. *The Dark Web dilemma: Tor, anonymity and online policing*. Centre for International Governance Innovation and Chatham House, 2015.

[39] Holly Johnson. Why doesn't she just report it? Apprehensions and contradictions for women who report sexual violence to the police. *Canadian Journal of Women and the Law*, 29(1):36–59, 2017.

[40] West Coast 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.

[41] Heidi Liu. When whispers enter the cloud: Evaluating technology to prevent and report sexual assault. *Harv. JL & Tech.*, 31:939, 2017.

[42] CH Logie, Ramona Alaggia, and Marie-Jolie 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.

[43] Helen Luce, Sarina Schrager, and Valerie Gilchrist. Sexual assault of women. *American family physician*, 81(4):489–495, 2010.

[44] Margaret J McGregor, Ellen Wiebe, Stephen A Marion, and Cathy Livingstone. Why don't more women report sexual assault to the police? *CMAJ*, 162(5):659–660, 2000.

[45] D Harrison McKnight, Michelle Carter, Jason Bennett Thatcher, and Paul 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.

[46] Enid Montague and Onur Asan. Trust in technology-mediated collaborative health encounters: Constructing trust in passive user interactions with technologies. *Ergonomics*, 55(7):752–761, 2012.

[47] David L Morgan. *Focus groups as qualitative research*, volume 16. Sage publications, 1996.

[48] Federal Bureau of Investigation. National incident-based reporting system. https://www.fbi.gov/services/cjis/ucr/nibrs, 2013.

[49] Media Kit on Sexual Assault. Media kit on sexual assault: Perpetrators. https://www.inspq.qc.ca/en/sexual-assault/understanding/perpetrators, 2020. Accessed: 2019-02-26.

[50] Community Ontario Ministry of Children and Social Services. Statistics: Sexual violence. http://www.women.gov.on.ca/owd/english/ending-violence/sexual_violence.shtml, 2020. Accessed: 2019-02-27.

[51] Samuel Perreault. Criminal victimization in canada, 2014. *Juristat*, 35(1):1–43, 2015.

[52] Anastasia Powell and Nicola Henry. Technology-facilitated sexual violence victimization: Results from an online survey of australian adults. *Journal of interpersonal violence*, 34(17):3637–3665, 2019.

[53] Martine B Powell and Rita Cauchi. Victims' perceptions of a new model of sexual assault investigation adopted by victoria police. *Police practice and research*, 14(3):228–241, 2013.

[54] Andrea Quinlan. Suspect survivors: Police investigation practices in sexual assault cases in ontario, canada. *Women & Criminal Justice*, 26(4):301–318, 2016.

[55] Brian A Reaves. Felony defendants in large urban counties, 2009-statistical tables. *Washington, DC: US Department of Justice*, 2013.

[56] Cristine 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.

[57] Cristine Rotenberg. Police-reported sexual assaults in canada, 2009 to 2014: A statistical profile. *Juristat: Canadian Centre for Justice Statistics*, 2017.

[58] Emily F Rothman, Deinera Exner, and Allyson 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.

[59] SARSAS. Coping with flashbacks. https://www.sarsas.org.uk/grounding/, 2020. Accessed: 2019-02-26.

[60] Sharon G Smith, Xinjian Zhang, Kathleen C Basile, Melissa T Merrick, Jing Wang, Marcie-jo Kresnow, and Jieru 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.

[61] Christina Underhill and Murrey G Olmsted. An experimental comparison of computer-mediated and face-to-face focus groups. *Social Science Computer Review*, 21(4):506–512, 2003.

[62] VESTA. Vesta social innovation technologies. https://www.vestasit.com, 2020. Accessed: 2019-02-27.

[63] Luis Von Ahn, Manuel Blum, Nicholas J Hopper, and John Langford. CAPTCHA: Using hard AI problems for security. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 294–311. Springer, 2003.

[64] James 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.

[65] Paul Willis. Learning to labour (London, Saxon House). *WillisLearning to Labour1977*, 1977.

[66] Jie Xu, Kim Le, Annika Deitermann, and Enid 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.

# Appendices

## A Participants' Demographics

| 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 2: Demographics of participants. SR, SW, I, and F represent survivor, support worker, interview, and focus group, respectively.

## B Saturation Graph

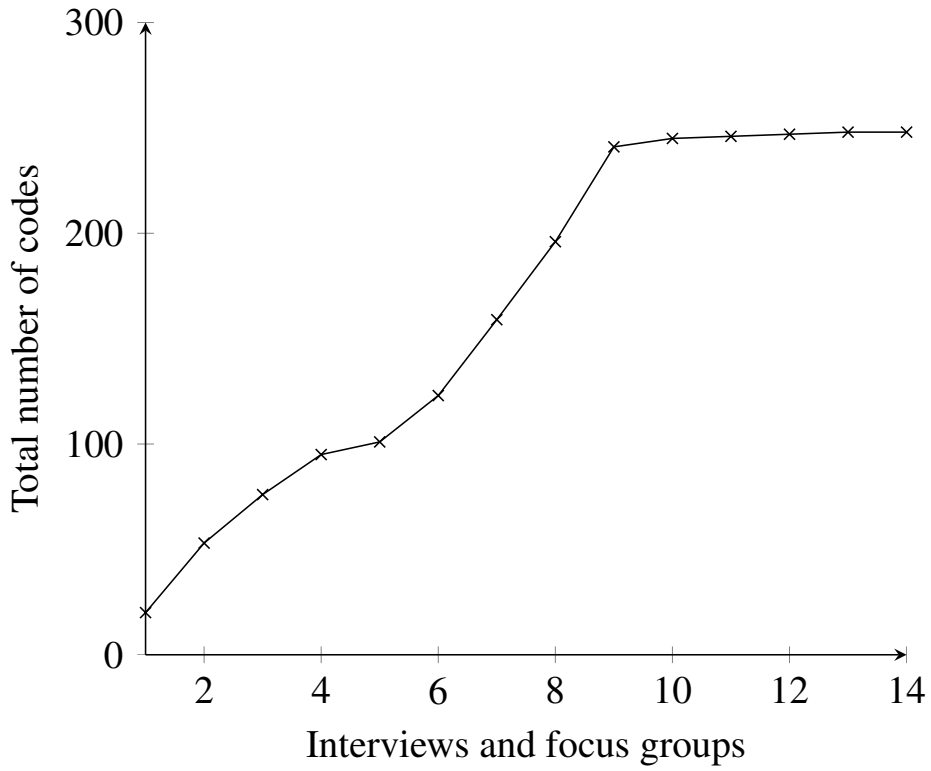



Figure 4: Number of codes after interviewing each participant

## C 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)

## D Sample of the O-TPRS Prototype Shown to Participants




Figure 5: O-TPRS Homepage

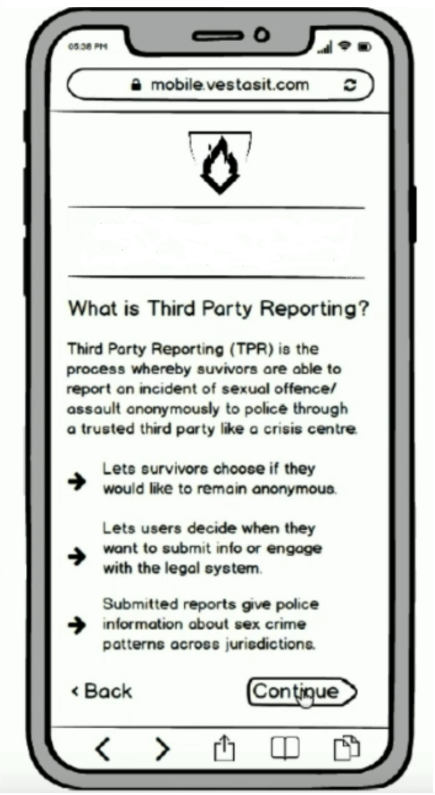



Figure 6: Introduction to TPRS




Figure 7: O-TPR Form Page 1




Figure 8: O-TPR Form Page 2

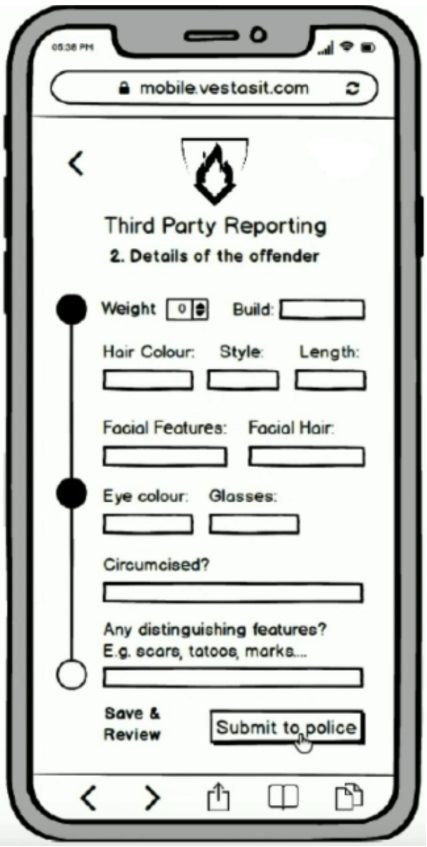



Figure 9: O-TPR Form Page 3

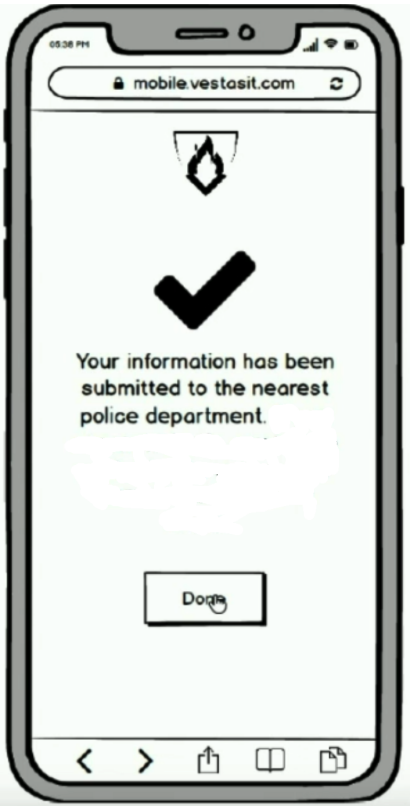



Figure 10: Submission Page