SoK: The Dual Nature of Technology in Sexual Abuse

Borke Obada-Obieh,* Yue Huang,* Lucrezia Spagnolo,† and Konstantin Beznosov*
*University of British Columbia, †Vesta Social Innovation Technologies
*{borke, huang13i, beznosov}@ece.ubc.ca, †lucrezia@vestasit.com

***Abstract*—This paper systematizes and contextualizes the existing body of knowledge on technology's dual nature regarding sexual abuse: facilitator of it and assistant to its prevention, reporting, and restriction. By reviewing 224 research papers, we identified 10 characteristics of technology that facilitate sexual abuse: covertness, publicness, anonymity, evolution, boundlessness, reproducibility, accessibility, indispensability, malleability, and opaqueness. We also analyzed how technology assists victims and other stakeholders in coping with and responding to sexual abuse. Our research questions examined the challenges in using technology to address sexual abuse too. For instance, its use by victims can lead to revictimization. To address technology's challenges, we offer recommendations and suggest new research directions. These findings about the dual nature of technology can inform research and development toward better support for victims of sexual abuse.**

I. Introduction

Sexual abuse is prevalent and destructive. One in every six American women and one in thirty-three American men are victims of an attempted or completed rape [1]. In Canada, one in three women will be sexually abused in their lifetime [2]. Sexual abuse violates a person's safety and privacy, and has long-term consequences, such as anxiety, depression, and suicide [3], [4].

The COVID-19 pandemic impacts the domain of sexual abuse in two major ways. First, sexual abuse has risen significantly during the pandemic [5]–[7]. Second, the pandemic also has accelerated the adoption of technology [8], [9]. Social distancing and national lockdowns have meant victims of sexual abuse have turned to technology for support, connection, community, and services. Unfortunately, abusers also have rapidly adopted this use of technology, amplifying the risks for victims. Since victims' reliance on technology is expected to continue beyond the pandemic, technological solutions are increasingly needed to connect them to services and to prevent, restrict, and report sexual abuse [10]–[12].

There is a need to understand how technology can be used to support victims without facilitating further abuse or increasing the risk of revictimization [13]. To better assist victims, the current gaps and challenges surrounding technological solutions must be understood because of the dual nature of technology in harm facilitation and harm reduction.

To this end, our aim was to provide a systematization of knowledge (SoK) on this dual use of technology. Our three research questions were: (i) What qualities of digital technologies might enable abusers to conduct sexual abuse more easily? (ii) What qualities of digital technologies might help address sexual abuse at the individual, organizational, and societal levels? (iii) What are the challenges with using technology to address sexual abuse? Answering these questions would help us identify the challenges in providing technological support to victims of sexual abuse.

We addressed our questions by conducting a literature review of 224 research papers. The selected papers discussed either how technology facilitates sexual abuse or how technology assists victims in preventing or reporting it. We analyzed the papers using a method proposed by Wolfswinkel et al. [14]

Our study has five major contributions: (i) We perform the first systematic review of knowledge on the dual nature of technology in both facilitating sexual abuse and assisting its victims. (ii) We identify 10 characteristics of technology that facilitate sexual abuse (covertness, publicness, anonymity, evolution, boundlessness, reproducibility, accessibility, indispensability, malleability, and opaqueness), and we analyze how these attributes facilitate the abuse of victims. (iii) We identify how technology assists victims and group the assistance into three categories (investigating, reporting or preventing, and restricting abuse). (iv) We offer the first-of-its-kind analysis of the challenges in using technology to provide much-needed support for victims of sexual abuse. Some of these challenges are related to a specific characteristic of the technology. For instance, the reproducibility aspect leads to the duplication of sexual content online. There are also other challenges not linked with any particular characteristic. For example, technological solutions for reporting or preventing abuse are poorly designed and maintained because of a lack of continuous funding or revenue. (v) We further discuss research ideas and solutions that can help navigate these gaps. We are optimistic these findings could lead to the development of better solutions for supporting victims of sexual abuse.

II. Definition of Terms

For the sake of clarity, we have defined the following terms:

Technology: A collection of systems "that allow users to exchange digital information over networks" [15]. We use *technology* as an umbrella term for all mobile, web-based, and Internet-enabled services, platforms, applications, and devices.

Sexual abuse: "Unlawful sexual activity and sexual intercourse carried out forcibly, or under threat of injury or with a person who is ... incapable of valid consent" [16]. We treat sexual assault and rape as particular types of sexual abuse. We

also use the term *abuse* for sexual abuse when the context is clear.

Perpetrator: "A person who carries out a harmful, illegal, or immoral act" [17]. Although there are different types of perpetrators, such as sexual perpetrators (rape, assault), perpetrators of economic fraud (sextortion) or perpetrators in the context of intimate partner violence (IPV) there is often crossover and even if they operate in distinctive ways, they are often conflated in the context of sexual abuse and are also referred to more generically as abusers. For reasons explained at the beginning of §IV, we have done the same. We use *perpetrator* and *abuser* interchangeably.

Victim: A person who has been sexually abused. We use the term *victim* in this paper; *survivor* can also be used. We acknowledge victims could be stakeholders, but we give them a separate category because of victims' importance.

Target: The person(s) a perpetrator aims to abuse sexually.

Stakeholders: The persons or organizations with a vested interest in supporting victims of sexual abuse. We use *stakeholders* to refer to frontline community agencies, law enforcement, and others providing economic, financial, or legal services for victims. (See also "victim.")

Revictimization: A victim's reliving of their sexual abuse either physically, emotionally, or psychologically.

III. Method

We used a five-step iterative process proposed by Wolfswinkel et al. to review the literature for our systematization of knowledge (SoK). Several peer-reviewed papers have used this method in their SoK [18]–[23]. This approach allowed us to reach a "thorough and theoretical analysis" of our topic and provide insights grounded in the literature [14]. The five-step iterative process itemized by Wolfswinkel et al. is (a) define, (b) search, (c) select, (d) analyze, and (e) present. We repeated between the steps as needed, since the process is meant to be iterative [14].

A. Define

In this step, we defined the scope of our literature review:

Inclusion criteria: For a paper to be included, it would have to satisfy all of the following criteria: (i) be a peer-reviewed journal article, conference or workshop paper, or book chapter; (ii) discuss sexual abuse; and (iii) discuss the use of technology to facilitate, report, or prevent sexual abuse.

Exclusion criteria: We would exclude papers that discussed sexual harassment (i.e., making rude, sexually degrading, or offensive remarks or gestures), not sexual abuse.

Selected source/database: We chose Google Scholar (scholar.google.com) as our source for papers because it provides a broad coverage of research topics [24]–[27].

Specific search terms: We would search using either the term *technology* or *social media* and combine it with each of the following: *sexual assault*, *intimate partner violence*, *IPV*, *human trafficking*, *abuse*. For example, technology human trafficking, social media sexual abuse.

B. Search

Using Google Scholar, we searched for papers using the terms we defined during the previous step.

While searching, we realized from the title(s) and abstract(s) of our results that we may unintentionally be omitting 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, identifying a total of 258 papers.

C. Select

The aim of this step was to check if the papers identified in the search (i.e., those found using the search terms) satisfied the inclusion criteria specified initially. For all of the papers identified during the search, we did the following review:

Citations: We checked forward and backward citations to see if any of the papers cited met our criteria. Through this process, we added 154 new papers, resulting in a total of 412 papers.

Duplication: We then filtered out duplicates (e.g., almost exactly the same paper but one version was published for a workshop, the other at a conference). After purging duplicates, we were left with 321 unique papers.

Criteria: We then read the full text of each paper in our dataset to determine if it met the inclusion and exclusion criteria. As a result, 91 papers were removed, leaving us with 230 papers.

Technological relevance: Of the 230 papers, 6 papers were from 1994–2004. After reading them, we decided to remove them because the type of technological tools described in the papers were no longer relevant (for instance, [28]). We ended up with 224 papers that we could use in this research, all published from 2005 to January 2021.

Two coauthors were involved in the first three steps. All authors were involved in the last step.

D. Analyze

During this step, we analyzed the papers in the selected sample. We analyzed our data in ascending order of publication date to see if specific trends emerged over time. As suggested by [14], we employed coding techniques as follows:

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 coauthors 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 resolve any disagreements. As a result, a total of 148 individual codes were generated.

Axial coding: Each of the two coauthors independently grouped codes identified during open coding into a set of categories. Then they met online to discuss the differences and converge on a single set of categories. Instead of quantitatively measuring the agreement between the two researchers, we focused on using the differences to discuss the best way to interpret the codes [29]. As a result, the researchers arrived at a set of 19 categories.

Selective coding: All coauthors 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 coauthors 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 categories and subcategories. We reached saturation in this process when no new revisions emerged.

E. Present

All coauthors organized the key insights that we derived from the categories and the relationship(s) between them. We present our findings in the following sections.

IV. Results: How Technology Facilitates Abuse

While digital technology alone cannot cause sexual assault, characteristics of its design can make harmful behaviors easier to perform. In this section, we present 10 such characteristics that emerged from our analysis of the literature: covertness, publicness, anonymity, evolution, boundlessness, reproducibility, accessibility, indispensability, malleability, and opaqueness. While performing the analysis, we also identified, whenever possible, the capabilities of the perpetrators that these characteristics enable or at least amplify. Our findings are visually summarized in Figure 1.

It is important to note that we did not differentiate the type of perpetrator for two reasons. First, it was often conflated in the literature. Second, we are presenting our results according to technological characteristics and not by the type of abuse or perpetrator. As such, to avoid confusion and added complexity we did not make the distinction.

A. Covertness

We defined *covertness* as the ability to operate technology in a particular location without the knowledge of the impacted individuals. This trait allows perpetrators to subtly gather information about or monitor their targets and victims. This is mostly seen in mobile or Internet of Things (IoT) devices [30], and spyware [31], [32]. Abusers can also hack into non-IoT devices, victims' emails, and social networking and media accounts (e.g., dating sites) to covertly use or gather information [33], [34].

Perpetrators use technological tools that enable the surveillance of another person but not vice versa. Chatterjee et al. [35] defined these types of technological tools as *subordinate tracking devices*. Perpetrators can misuse these tools to gather information about their victims covertly [36]. For example, Westmarland et al. described Track Your Wife, a mobile app that runs in the background of the device where it is installed. The app periodically sends the time and the device's geolocation to a server. Using this information, a perpetrator can know the device's location (and, in other words, the location of the victim) [37]. Another example is the use of auto-answer phones with the ringer set on silent. These types of phones automatically answer calls. Perpetrators can leave auto-answer phones in victims' cars, houses, or other locations, and call the phone to listen in on victims' conversations without their knowledge. Using the information from these calls, perpetrators can determine the recent activities of victims and plan a suitable time and place to abuse them [38], [39]. Perpetrators can also use parental apps and track-my-pet types of apps to monitor their victims [40]. Further, perpetrators can use spyware [31], [32], [41]–[45], such as screen, audio-visual, and voice-activated recorders [46].

Perpetrators use personal and mutual tracking technologies. Chatterjee et al. defined personal tracking apps as those that are "intended for use solely by the owner of a phone" (e.g., find-my-phone types of apps) and mutual tracking are "apps that allow a group of people to track each other's locations" (e.g., apps to track family members) [35]. For example, the location of victims who are fleeing from perpetrators to various shelters can be revealed by the GPS technology of their mobile devices [47]. Many studies report various means by which perpetrators misuse both personal and mutual tracking apps to monitor victims discreetly [32], [35], [39], [40], [43], [48]–[69]. Perpetrators can also surreptitiously use other technologies for surveillance, such as IoT devices [70]–[76], hidden cameras [36], [37], [39], [40], [42], [46], [48], [55], [67], [77]–[83], and many other types of technological tools [35], [40], [44], [54], [56]–[65], [67], [83], [84].

Tracking functionalities are available by default on some technological devices, providing more avenues for victim surveillance. Tracking functionalities are provided within a device's operating system or by the service provider, which means users cannot uninstall these apps. Chatterjee et al. outlined that "Android natively provides tracking functionality via Find My Device, or via Google Maps' unlimited location sharing functionality. Assuming that 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" [35].

Apart from surveillance, perpetrators can subtly compromise victims' online accounts to impersonate them or use their information. Researchers reported incidents where abusers had garnered information about their victims from their compromised accounts without their knowledge [77], [80]. Fraser et al., for instance, described the case of a police officer who wanted revenge against his ex-girlfriend and gained control of her email account. The officer used her email to impersonate her on a dating site and arranged for 70 men to meet up at her home [77].

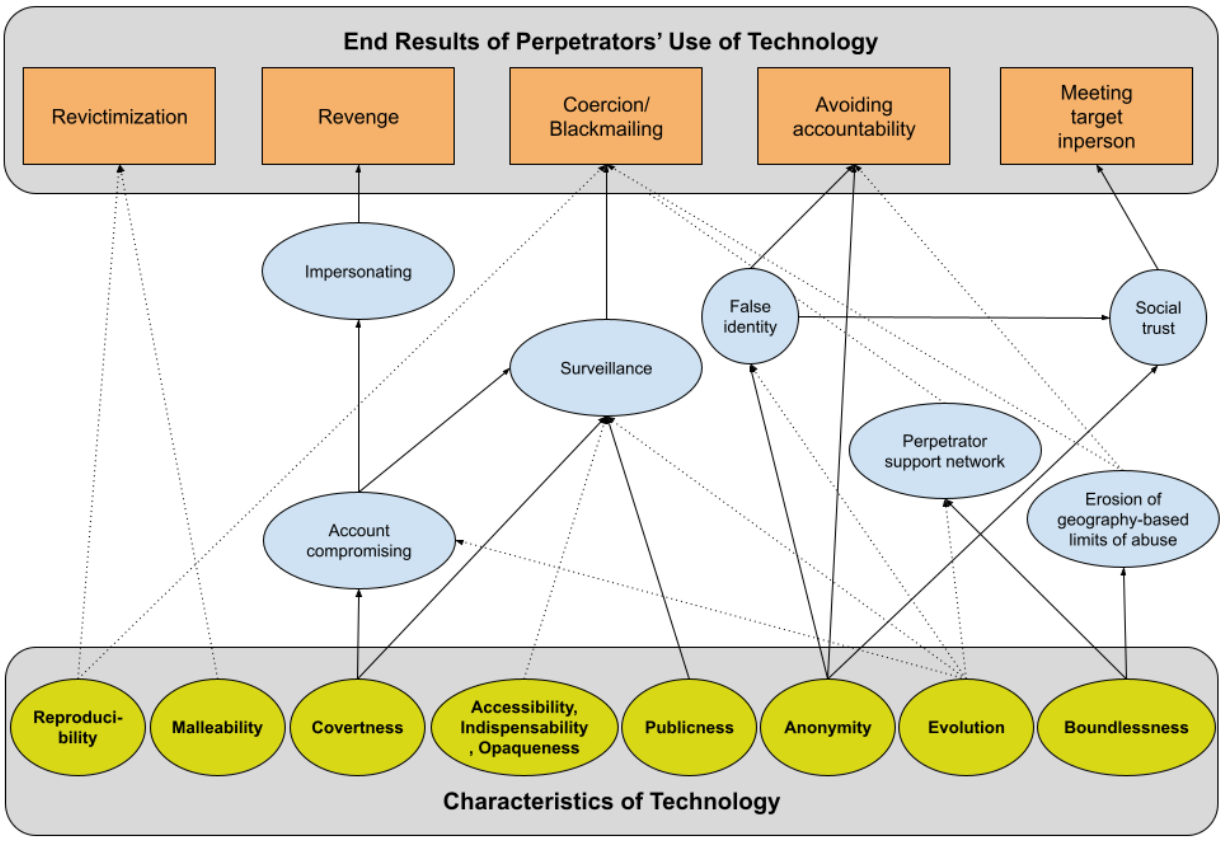

Fig. 1: Visual summary of how technology facilitates abuse (§IV). Solid lines indicate specific characteristics that enable perpetrators' capabilities, whereas dotted ones indicate amplification.

The covertness trait creates a Big Brother effect, whereby the perpetrator always has up-to-date information about the victim and can have the upper hand over them. Because of how discreetly technology is used, victims may not know about abusers' activities [33], [37], [77], [80], [82], [85], [86]. The omnipresence and omniscience effect makes it hard for victims to distance themselves from perpetrators, which leads to more opportunities for abuse [77], [82].

Perpetrators coerce victims to indulge in sexual acts because of the sensitive information perpetrators have about them. Perpetrators can gather a significant amount of information about victims, including sensitive surveillance videos, images, or audio recordings. To sexually abuse victims, perpetrators can blackmail victims by threatening to share sensitive information obtained from covertly monitoring them [42], [52], [67], [82], [87]–[89]. Because of the fear that the perpetrators will make good on the threat, victims keep engaging in sexual acts with the perpetrators [90].

B. *Publicness*

In most cases, information kept on the Internet is public. Unlike covertness that deals with collecting nonpublic information about victims, *publicness* refers to publicly available information that is created when a person uses technology.

Perpetrators use social media sites to gather information about targets or victims. Much personal information is displayed on social networking and media sites. Through these platforms, perpetrators can learn about their targets' likes, dislikes, interests, geolocation, school or workplace, and other personal information. Perpetrators can then use the information to build an online relationship with their targets and proceed to off-line meetups to sexually abuse them [32], [39], [40], [44], [67], [77], [82], [91]–[94]. Perpetrators can also learn current information about their past victims to facilitate the continuation of sexual abuse [50], [82], [93], [94].

Victims find it challenging to avoid perpetrators monitoring them using their publicly available information. Many researchers report this challenge [32], [47], [82]. Sometimes the perpetrators are still friends or connected to the victims' friends or others in their networks on social media and other online platforms. Therefore, the perpetrators can use these platforms to get current information about the victims (e.g., the victim's location and activities) through their friends on social media. The perpetrator can use this information to locate the victim and continue the sexual abuse [52], [82]. Further, victims living in shelters have difficulties hiding their exact locations from perpetrators because of publicly available social media information. Matthews et al. explained

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]." The paper further reported that to stop perpetrators from using victims' publicly available information, victims had to restrict their children's social media activities or block mutual friends the victims have with the perpetrators [32].

The default settings of websites make information publicly available. Using some online platforms can lead to the disclosure of information that people do not want made public [32], [52], [67], [69], [77]. For instance, Facebook allows people to tag other users in posts or photos by default [95]. This can help abusers determine their targets' locations or recent activities their targets have engaged in. Users would have to manually change these settings.

Some apps facilitate the aggregation of publicly available online data. Such aggregation can be useful to perpetrators. Dimond et al. discussed an app, Google Buzz, which collated people's online identities from various websites. The authors explained: "When Buzz launched, it disclosed all the names of Gmail contacts publicly. 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" [93]. Perpetrators have exploited similar apps [42].

C. Anonymity

We defined *anonymity* as the ability to hide one's true identity when using technological tools. Anonymity comes in various forms when using the Internet or cellular devices.

Perpetrators can create false identities that facilitate in-person meetings with targets [90], [94], [96]–[98]. The Internet helps people hide under many layers of anonymity. For instance, the Tor Internet web browser facilitates the protection of people's identity online by providing a secure network for communication [99]. Perpetrators can create a false online persona that people would most likely find appealing and engage with [91], [94], [100]. Multiple papers reported incidences where the Internet facilitated anonymous grooming of targets and eventual in-person meetings [90], [101], [102]. Further, perpetrators can make multiple false identities by creating many online accounts and profiles on websites [88], [91], [101]–[103].

Perpetrators build social trust between themselves and their targets. Social media is built on the network and concept of friendships [104]. The anonymous friend feature of several social networking sites helps victims trust perpetrators. Being friends with strangers on some social media platforms can make people assume they know a stranger when, in reality, they do not [96]. Kloess et al. noted that the constant anonymous communication on the Internet helps "foster feelings of belonging and a sense of community to form relationships and build friendships" [94]. Victims reported increased friendliness or a false sense of knowing perpetrators online before they met in person [91], [96], [105]. Similarly, the idea of social trust can be seen in dating sites and apps. Perpetrators create false online personas to build trust with their targets [77], [80], [90], [106]. People can be more emotionally vulnerable on dating sites and trust an appealing stranger more easily [80], [107].

Further, perpetrators can use a combination of technological platforms. For instance, while the initial meeting could be on a social media platform, the abuser could continue the conversation using other technologies (e.g., text messages and calls) to build social trust [91], [94], [103], [105], [108]–[110].

Anonymity and a heightened sense of social trust lead to eventual in-person meetings. Perpetrators exploit the false sense of connection, relationship, and trust provided by these sites to facilitate off-line meetings and the sexual abuse of targets [80], [90], [91], [98], [103], [105]. The idea of confidence and social trust is similar to the literature on how con men gain their victims' trust through confidence games (also known as *cons*) [111]–[114].

It is difficult to hold a perpetrator accountable. Complex layers of anonymity, such as the encryption of online communications, make it difficult for law enforcement to identify and apprehend perpetrators [115]–[117]. In addition, the multiple technological tools used by perpetrators each have their own layers of anonymity, adding to the difficulty of apprehending perpetrators [42], [116]. Awareness of these challenges can develop perpetrators' confidence and, therefore, a continuation of the crime of sexual abuse [118].

D. Evolution

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

Advances in technology are being weaponized. While the evolution of technology is essential, it expands the perpetrators' repertoire [77], [96], [98], [119], [120]. Tools are used in ways that were never intended, and perpetrators weaponize technological evolution to scale up their offenses [37], [48], [68], [87], [103], [121]. Perpetrators use various online platforms to facilitate the distribution of unauthorized sexual recordings [115], [122]. Real-time instant messaging services increase the speed of communication between targets and perpetrators [119]. Search engines, chat rooms, emails, online dating sites, and mobile phones can aid perpetrators in locating targets [79], [80], [90], [94], [97], [102], [103], [107], [119], [123], [124]. Spyware and multiple IoT technologies can be used to monitor targets and victims [30], [40], [70], [77], [91].

Perpetrators adapt as technology evolves. Many research papers illustrated various ways perpetrators have adapted when technological abuse tools are modified or taken away from their toolbox [68], [103], [121].

E. Boundlessness

Boundlessness refers to technology's lack of geographical barriers. It is not confined to a particular location. This trait is mostly seen in Internet-based technologies.

The Internet's boundlessness trait makes it easier for perpetrators to form ties with other perpetrators, share tips and

strategies, and strengthen their network [96], [110]. Before the Internet, such support and collaboration among perpetrators would have been impossible [80], [91], [103], [110]. This trait allows for more like-minded people to come together on online platforms with the goal of bonding, exchanging sexual fantasies, identifying tools to aid surveillance, and facilitating online and off-line sexual meetups with targets or victims [100], [103]. Perpetrators use these communities to get others interested in being part of sexual crimes. Kloess et al. explained: "In terms of offending behavior, such communities may also have changing effects on users' views due to its support and understanding, as well as justifying and normalizing features" [94], [96].

Further, technology's boundlessness opens up more opportunities for perpetrators to meet more targets from many physical locations [100], [125]. Technology gives "expanded access to victims for offenders" [117]. 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" [117].

Perpetrators can continue the abuse of an ex-partner and blackmail them due to boundlessness. The abuse can continue long after the relationship has ended. When in a relationship, people may share their online space. However, after their physical relationship has ended, ending their online relationship can be complex [67]. Hand et al. explained that, because of technology, "geographic and spatial boundaries no longer present a barrier for one to communicate, contact, or locate another globally" [69]. 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" [41]. Sometimes abusers still have access to victims' previously shared online accounts and can use the account information to blackmail the victim into engaging in sexual acts [55]. Technology, therefore, "lessens [the] personal sense of privacy boundaries" [50].

F. Reproducibility

Reproducibility is the ability to duplicate information kept on the Internet, making the information close to permanent.

Sexual content shared online is easily duplicated, resulting in revictimization. Perpetrators share sexual images, videos, or audio recordings of victims on the Internet, where it is easily reproducible and close to indelible [60], [87], [88], [90], [101], [102], [115], [126]–[137]. Many research papers document the difficulties victims face in attempting to remove content that has been reproduced on various online platforms [87], [91], [102], [137]. In situations of unauthorized duplication and distribution of sexual content, victims have described feeling as if the sexual abuse was occurring all over again [90], [100], [137]–[139].

Because of reproducibility, perpetrators can also blackmail victims. Perpetrators can coerce victims into engaging in sexual activities by threatening to share sexual content online if victims refuse or report the incident to the police [48], [88], [91], [98], [119], [140]. Afraid the perpetrator will make good on their threat and that their sensitive information will be visible online forever [80], victims continue sexual interactions with perpetrators [90], [106], [117], [128], [140]–[142].

G. Accessibility

Accessibility refers to technology being easily available to multiple individuals. As a result, perpetrators do not have to be sophisticated technology users to employ technology for sexual abuse. "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" [48]. The increased accessibility of technology enables easy monitoring and abuse of targets and victims [91].

H. Indispensability

The indispensability of technology makes it essential in everyday life, increasing people's reliance on technology and enabling perpetrators to have access to victims consistently as a result.

The use of technological tools and platforms has become a necessary part of people's lives [40]. 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 [94], [123]. Some sexual abuse shelters request that victims do not use technology in order to prevent perpetrators from tracing them to their current location or to shelter facilities. However, victims find this request hard to adhere to [143]. People have become so dependent on technology that they find it challenging to cut themselves off from it, even if it comes at the risk of sexual abuse [91].

I. Malleability

Malleability refers to how easy digital content can be tampered with. A picture can be photoshopped; video and audio content can be altered using artificial intelligence. Perpetrators circulate modified sexual content of victims to facilitate revictimization [90].

J. Opaqueness

Opaqueness refers to a system with contents that are mysterious to the user. In our case, the system is technology.

The type and volume of user data collected by technological devices is unclear, and perpetrators use this lack of clarity to their advantage. For instance, victims in a research study complained 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 [70]. Because the technological device is opaque to victims, perpetrators make use of the device to continue surveillance of victims [51], [74].

Further, victims did not know details about the accounts they shared with the perpetrators, making it easy for the perpetrators to continue to access their accounts. This opaqueness

made it difficult for victims to cut ties with their abusers; in turn, the perpetrators continued to surveil and blackmail victims using their shared accounts [58].

V. Results: How Technology Assists Victims

In this section, we present the ways in which technology assists victims. We classified the assistance into three broad categories: (a) investigating abuse, (b) reporting or preventing abuse, and (c) restricting abuse. We discuss how technology can assist victims. Importantly, we also describe the challenges (summarized in Figure 2) that hinder this assistance.

A. Investigating abuse

Digital files kept on technological tools and platforms can serve as evidence of sexual abuse to aid investigation [144]. We classified such evidence into two categories: (i) evidence that captures the act of sexual abuse, such as images, videos, and audio files; and (ii) evidence of the perpetrator's actions that facilitate the abuse, such as monitoring or stalking the victim. Such evidence could include online posts, text messages, and records of phone calls. For simplicity's sake, in the rest of the paper we refer to these categories as sexualabuse_evidence and preparatoryactivities_evidence. We use the term *evidence* to refer to both categories.

Perpetrators and witnesses can record the sexual abuse incident, which serves as sexualabuse_evidence. Technological platforms like Twitter, Facebook, or YouTube can enable people to record and post real-time events [145]–[147]. These recordings can serve as a digital record, showing that the sexual abuse occurred. It is also easy to screenshot or otherwise save such recordings. Therefore, the evidence can remain, even after it has been deleted from an online platform [50], [58], [91], [144].

Such evidence has been helpful to victims in their pursuit of justice [50], [91], [144]. Sometimes victims were unaware they had been raped. For instance, in the Steubenville sexual abuse incident [126], the perpetrators and complicit witnesses recorded the repeated sexual abuse of the victim. The recording was documented through videos, images, text messages, emails, and online posts that were uploaded on Facebook, YouTube, and Twitter [126]. However, the victim did not know that she had been raped because she had been in and out of consciousness at the time. Seeing the videos and posts online made her realize what had happened [126]. The perpetrators took down the images and videos before the police investigation started weeks later [148], but screenshots taken of the original postings helped to serve as evidence. There are also many other instances where perpetrators had made off-line video recordings of themselves committing sexual abuse crimes. The police discovered these video recordings during their investigations and used them as evidence of sexual abuse [78], [144], [149].

Victims can also record sexualabuse_evidence. They have used their mobile phones to serve as witnesses to the crime of sexual abuse. For instance, a victim who was being abused dialed the emergency number under the bedcover, hoping someone would listen in and piece together what was happening [41]. In other instances, victims have recorded incidents [91] or called family and friends while being sexually abused to make them listen in as evidence of the abuse [41], [50]. Victims have taken pictures or videos of specific injuries they had after sexual abuse happened [90]. Further, victims have saved text messages or social media posts from abusers that insinuated sexual abuse had happened [86], [91], [150]. Victims have used such evidence to get a restraining order against abusers [32] or for investigative purposes [50], [91], [150].

Online evidence also facilitates digital activism. Joyce defined digital activism as a "political campaigning practice that uses digital network infrastructure to pursue social change" [151]. Victims can use evidence for digital activism with the hopes of getting justice [58], [152], [153]. For example, digital activism was used in the Steubenville's case "to hold those in power accountable online in ways that bypass official justice mechanisms" [148]. Sometimes victims have used social media to tell their stories, which can aid digital activism [129], [154]. Seeing victims share their stories online has been a motivating factor for other victims to share their stories as well [129], [152].

1) ***Challenges with using technology to investigate abuse:*** Here we present the challenges that stakeholders and victims experience when using technology to investigate abuse, both during and after the gathering of evidence.

During the gathering of evidence: It is hard for stakeholders to collate evidence because of multiple sources and large volumes. Sometimes the perpetrator communicates with the victim on more than one platform. For instance, a conversation could start via instant messenger and then lead to email exchanges or conversations using other technological platforms. It is also difficult to provide preparatoryactivities_evidence of communications with the perpetrator because of the sheer volume of evidence accumulated on various technological platforms [91], [108], particularly in cases of long-term abuse [79].

It is difficult to get the consent and timely cooperation from various service providers to access evidence that the victim could need in a court of law [91], [108]. The service providers can be unresponsive or slow to release the information, and the process can take many months [79], [91], [128]. In some cases, victims waited for a long time and eventually withdrew their sexual abuse reports because they believed they were not getting justice [155]. In other cases, the service providers did not keep records of the evidence that the victims or law enforcement agencies were looking for or did not release the information because of privacy concerns [91].

Another challenge is that it is the victim's responsibility to gather evidence, which can be a difficult task. Evidence gathering is necessary for finding justice [155]. However, victims are expected to gather evidence, which puts the responsibility and onus on them. For instance, regarding preparatoryactivities_evidence, "many jurisdictions suggest that victims keep a stalking log to document each stalking incident. By noting the date, time, location, means of contact, and witnesses" [77].

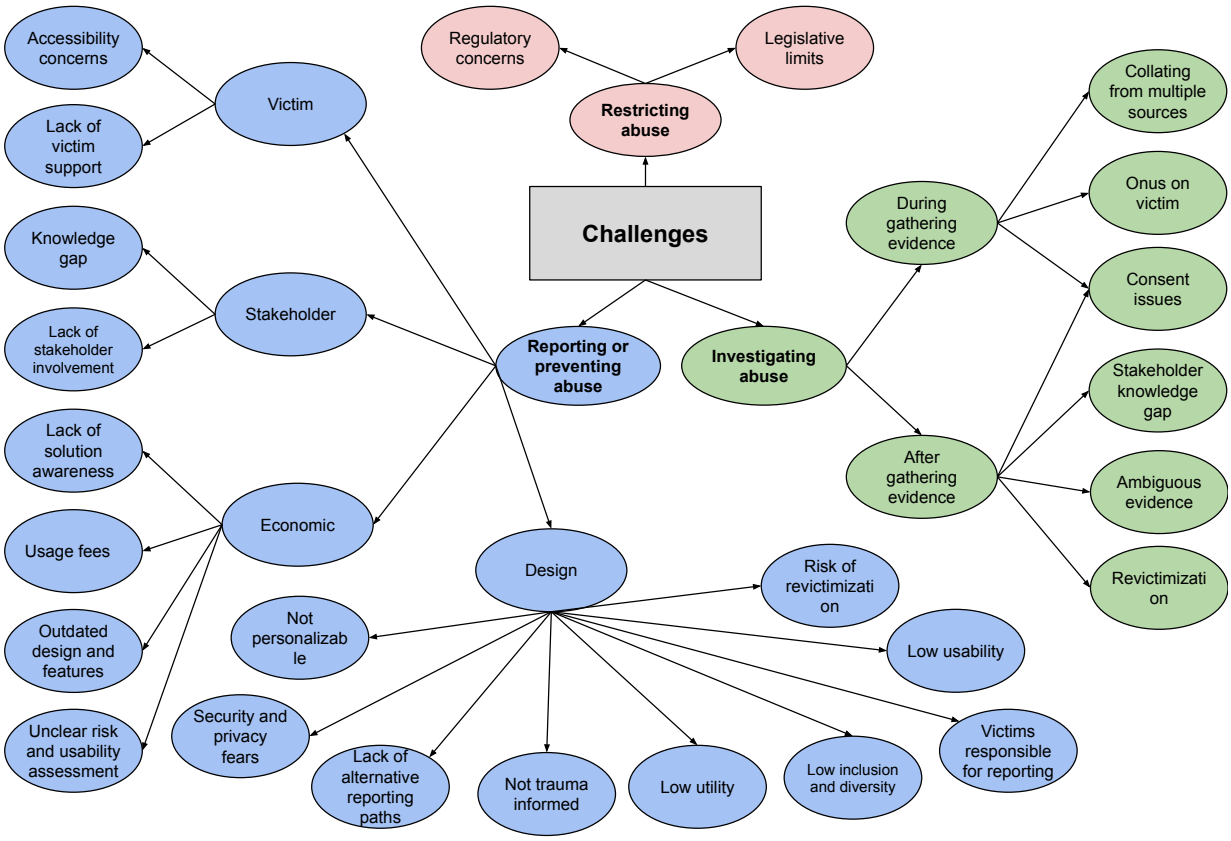

Fig. 2: Visual summary of challenges with using technology to assist victims (§V)

Further, in the court of law it is mostly a case of the victim's words against the perpetrator's. Victims, therefore, must gather as much evidence as they can to prove that the perpetrator is guilty [58]. Such gathering of evidence is often done at the risk of the victim's life or with the risk of revictimization [58].

It is also unclear if consent is required to gather evidence that will be admissible in court. Evidence gathering is done discreetly without the perpetrator's knowledge. For the evidence to be admissible in court, it is unclear to a victim if they require the perpetrator's consent to gather such evidence [78]. For instance, regarding sexualabuse_evidence it is often unclear if the victim needs consent from the perpetrator to record the incident since both parties were involved in the act [58].

After the gathering of evidence: Victims can be revictimized. Some perpetrators have recorded themselves raping their victims and uploaded the content online. This digital content can serve as sexualassualt_evidence and help victims get justice. However, the knowledge that such content exists, and could be duplicated and replayed multiple times, can be very traumatic for victims [96], [102], [126], [136]. Such evidence serves "as a constant reminder of the abuse and suffering, perpetuating humiliation" [80]. One such incident is the tragic case of 17-year-old Rehtaeh Parsons. Multiple perpetrators sexually abused Parsons when she was 15 years old. During the incident, a photo was taken that was then circulated on social media. Even though the picture acted as evidence of the crime, it also resulted in cyberbullying and psychological revictimization, and eventually led to Parsons committing suicide [137].

Another challenge is that preparatoryactivities_evidence can be ambiguous. Occasionally collected [86], this category of evidence can include the accumulation of activities illustrating that the perpetrator intended to abuse the victim sexually at a later time. However, such evidence can be ambiguous, difficult to collect, and difficult to determine if it proves a person's plans to commit sexual abuse [51], [79]. It is therefore easy to discard such evidence [78]. For instance, "victims would attempt to seek support by reporting the technology-facilitated abuse to the police or discuss it with a trusted contact, only to be told that the devices may be malfunctioning or that the victim does not know how to use them correctly. [Stakeholders] also demonstrated concern over the 'believability' of such cases, wondering whether they themselves would find accounts of smart homes being used for abuse credible" [74]. Many victims have had to endure technology-facilitated abuse from perpetrators until it reaches a measureable extent before the justice system can intervene [77].

Stakeholders' knowledge gaps also leave victims at risk. Some law enforcement officers and support workers lack an adequate understanding of technology or its facilitation

of abuse [48], [58], [90], [155]. Stakeholders' knowledge gaps in this area put victims at more risk by limiting the number of victims that come to seek help [58], [90], [128]. Sometimes frontline police officers (who should be victims' first point of contact), support workers, and judges do not understand the technology-facilitated abuse that victims are reporting or the extent of the harm that technology can cause if misused [128], [136], or they have insufficient knowledge of technology-related abuse to help victims [79]. Further, the rapid rate at which technology is evolving widens this knowledge gap [155]. Stakeholders identified the challenge of keeping up with technology development as the most difficult part of collating and using evidence [155]. Even before interacting with the new technologies, stakeholders believed new technologies were complex to use [43]. Stakeholders also admitted to not knowing the right questions to ask victims about technology-facilitated abuse because of the knowledge gap [79].

There are misconceptions about what technology can or cannot do, limiting the believability of evidence. Stakeholders have no clarity on the limitations or capabilities of a particular technological tool, meaning they can overestimate or underestimate what technology can do. For instance, some stakeholders believe all technology shown in movies or on TV is possible in real life, which may not be the case [77].

After gathering evidence, it is still hard to determine if consent was given. The determination of consent is a crucial part of the investigative process in courts [155]. While in some cases digital evidence clearly shows the absence of consent, in other cases it is hard to determine [144]. It is even harder to determine if consent was given and revoked later [91], [138].

It is also difficult to prove that a person committed sexual abuse. Because of how malleable technology can be, it is hard to determine if a person committed sexual abuse based on digital evidence. For example, "there are significant challenges for police in proving who created, shared, or threatened to share, an image: How do you prove that that particular Facebook account is operated by the defendant?" [128].

B. Reporting and preventing abuse

Technological solutions can assist victims in two major ways: giving them a platform to (i) report and (ii) prevent sexual abuse. For the rest of the paper, we refer to technological solutions as *solutions* when the context is clear.

Many types of solutions exist for victims, support workers, and bystanders. As Cardoso et al. put it, solutions range from "jewelry that provides location information to family and friends, ... [to] underwear that shocks potential rapists" [56]. Various solutions have been developed by industry and government to help victims report and prevent sexual abuse, (e.g., helplines, educational online resources, online forums and support groups, educational campaigns, and various apps for mobile devices) [48], [50], [62], [68], [90], [100], [105], [117], [121], [125], [136], [156]–[164]. Other solutions focus on changing perpetrators' behavior and on educating the public to be ethical bystanders [42], [87], [105], [133], [141], [165]. Academic researchers have also put forward a number of proposals [36], [68], [76], [118], [156], [158], [166]–[175].

*1) **Challenges with using solutions to report and prevent abuse:*** Here we present the challenges of using technological solutions to report and prevent abuse. We categorized them into design, stakeholder, victim, and economic challenges.

Design: Solutions are designed to have one path of reporting. Sometimes, however, victims cannot or are unwilling to take that path, but they are not given other alternatives. For instance, reporting solutions do not prevent reports of victims from being accessed by local police officers if the latter happens to be the perpetrator [43].

Some solutions lack utility and do not serve a practical need in real life [176]. For instance, stakeholders "were largely critical of panic alarm/danger alert style apps ... they did not really 'add' anything—that a quick text to the same effect could easily be sent or information quickly searched for online" [160].

Solutions have low inclusion and diversity. They are developed with a stereotype mentality [56], [157]. For instance, some seemed to have been developed with the assumption that all users in a household trust each other [51] or have harmonious family relationships [93]. Other solutions require victims to have unrestricted and complete access to a technological device, which is not always the case [37]. Researchers advocate for a more inclusive design that considers various abuse stages for victims [56], [118], [157].

Preventive solutions put much of the burden on the victim, which reinforces victim blaming. Solutions for preventing abuse are focused on a series of activities that victims must do to keep safe [42], [56], [80], [177]. Such solutions put the onus on victims to ensure their safety [37], [157] and reinforce rape myths [80]. Some solutions require victims to alter the way they use technology in order to protect themselves [56], [165]. Mason et al. explained: "Such [technological] applications are aimed at women as needing to be responsible for violence, rather than ... initiatives that would target perpetrators of violence. ... women are problematically expected to change their behavior by tracking their whereabouts and 'checking in' with friends to prevent violence. [The solutions] ask women to give up personal information to third parties for their own self-protection" [39]. Putting such a burden on the victim can "ultimately reproduce unhelpful victim-blaming narratives and may have the effect of promoting fear and timidity in using technology" [42].

Solutions can have low usability. Solutions' usability is critical, especially because victims may be at a higher level of stress, risk, and vulnerability when using them [32], [68]. Some solutions had poor usability [48], [160], and may be too technical for an average user [157], [173], [174].

There are also security and privacy concerns about solutions [178]. Rodríguez et al. proposed using telemonitoring devices for victims of intimate partner violence [168]. However, "[telemonitoring tools] can improve [victims'] safety, but also imply recording personal data, wearing smart devices, and allowing text and voice recognition software, and this could

be considered interference in a private life. This could lead to a rejection of the technology by the survivor" [156].

Victims can be revictimized if perpetrators discover they are using the solutions. Many papers discuss the risk of the perpetrator seeing the victim researching online resources or using other technological solutions, resulting in the perpetrator revictimizing the victim [41], [50], [67], [68], [93], [121], [125], [156], [178].

Another design challenge is solutions that do not work or are not trauma informed. Brignone and Edleson [160] surveyed several smartphone apps in the app store and discovered that some apps do not fulfill their claims. The researchers also found that the design of some apps is not trauma informed (e.g., containing information that blames victims for the abuse).

Solutions that cannot be personalized are also a challenge. Stakeholders and victims have a wide range of technical expertise [67]. Further, victims are in different abuse stages [48]. Solutions ideally should account for those differences [43], [48]. Research suggests that a single solution or a one-size-fits-all approach will not help victims [58], [179]. Personalized solutions or a combination of solutions are needed [68], [160].

Stakeholder: Stakeholders fear that, despite the precautions in place, perpetrators may still discover that the victim is using a solution, resulting in revictimization [180]. Therefore, some stakeholders refuse to recommend the solutions to their clients [48], [180]. Further, some support workers did not fully understand the technological solutions, and they "simply wanted the technology to go away" [78]. Support workers admitted they had low technological readiness and lacked the time to learn about the solutions [43].

Another stakeholder challenge is a lack of involvement in the development of solutions [116]. Solutions are developed in isolation without them [37], [45], [161]. This lack of involvement leads to the design of solutions that do not assist victims [79], [161], [178] and that stakeholders are unwilling to use [30], [51], [86], [157], [174].

Victim: Victims have accessibility concerns. In describing the limitations that victims face, Stonard et al. explain that "those least likely to use the Internet for assistance will be those who tend to be most marginalised; this includes women who are refugees, women whose first language is not English, women who are not literate, and women in poverty who have no access to the Internet or do not have the requisite skills for using the Internet" [67]. Solutions are not accessible to victims with literacy and language barriers [67], [118], [167], [169], [174]. Further, most trafficked victims do not have smartphones to download the apps or use the solutions [43], [125].

Victims also can need in-person support. While using technological solutions, some victims need a support worker to be present either on the phone or in person to help them [169], [181]. Research also suggests that, regardless of the solutions, they could never replace face-to-face interactions [43].

Economic: Solutions are poorly marketed, so victims and stakeholders do not know about them or where to find them. For instance, the research of Westmarland et al. suggests that stakeholders "had not worked with any woman that said they had used a domestic or sexual violence app" [37]. Stakeholders interviewed in another study had never heard of the apps designed for preventing or reporting sexual violence [160]. Further, victims that need to use the solutions do not know they exist [48], [68]. In a study by Bouché et al. [121], over 70% of the victims said they never saw any hotline number they could use to dial for help. Also, the majority of the victims admitted that while they wanted help escaping from their abusers, they did not know where to get it or how to seek it out [121]. Victims had contacted support centers for help, but those centers lacked the needed information or recommendations [54]. In addition, while surveying sexual abuse apps in the app store, Brignone and Edleson [160] discovered that most of the apps lack visibility even in the app store. Cardoso et al. also noted that in situations where solutions are marketed, there is little or no evidence of what the solutions claim to do, which can discourage victims from using the solutions [56].

Unclear usability testing or risk assessment is another economic challenge with using solutions to report and prevent abuse. It is unclear which of the proposed and developed solutions are evaluated to avoid low usability or risk to victims [37], [160]. Developers also do not explain to victims the safety risks associated with using the solutions, creating a false sense of security [37], [174]. Such knowledge would help victims to gauge their environment and safety and decide if the solution would be appropriate.

The solutions are also improperly maintained and/or outdated [83], [160]. Maintenance of the solutions is critical to ensure that the solutions have up-to-date information and security where needed [160]. However, the developer may not have the time and resources for maintenance [43], [83].

Some solutions charge fees, which can seem exploitative. As explained by Mason et al., "companies are primarily concerned with developing tools that consumers will purchase rather than with women's safety" [39]. A pay-as-you-use business model is challenging in the domain of sexual abuse prevention and reporting, as victims are not willing to pay for such solutions and view those solutions as "exploitative" [56], [125], [157].

C. Restricting abuse

Service providers have put in place some technological measures to restrict abuse. For instance, some social media sites have methods to flag pornographic content on their sites [100]. Some organizations have customized their technology (e.g., Google Maps hides undisclosed victim shelters [39]).

Governments have also implemented measures to restrict abuse. For example, some countries in Asia have implemented Internet filtering to limit social networking and websites that carry pornographic material. This limitation is to reduce the possibility of sexual abuse grooming and psychological revictimization [100], [123]. Some laws also require that social media sites close the accounts of any found sexual perpetrator [100] and attempt to find the perpetrator's location [50].

Further, countries have laws that help to limit the use of surveillance devices against victims [138]. Governments have also legalized the use of drones by government officials to monitor sexual abuse activities of sex trafficking perpetrators [78].

*1) **Challenges with restricting abuse**:* Here we present the challenges of using technological solutions to restrict abuse. We categorized them into regulatory concerns and legislative limits.

Regulatory concerns: Finding a balance between monitoring sex traffickers and protecting people's privacy is difficult. Governments in some cities use drones to monitor sex traffickers' activities, but the use of drones invades people's privacy [78].

Legislative limits: Most laws on sexual abuse are not uniform across jurisdictions, making it challenging to apprehend perpetrators [138]. Perpetrators could meet a target and commit sexual abuse in one state while living in another where some of these laws do not apply [62], [90], [128], [138].

VI. Discussion

A. Limitations

Our SoK centered mainly on research work in developed countries, which may have influenced our categorization of technology's attributes. However, most of the research papers we found in the field of technology-facilitated sexual abuse centered on developed countries. Further, we do not specifically focus on the link between technology and child sexual abuse.

As with any qualitative research, our findings may have been affected by systematic biases [182]. To reduce researcher bias, multiple researchers were involved in analyzing the data and converged on their interpretations [26], [27]. 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 [24]–[27].

Despite the above limitations, we believe our study provides a helpful background for future research on using technology to assist victims and reduce sexual abuse.

B. General discussion

The goal of our paper was to identify the gaps in technological assistance for victims of sexual abuse. Our findings point to the characteristics of technology that facilitate abuse (Figure 1) and also to gaps in investigating abuse using digital evidence, reporting and preventing abuse using technological solutions, and restricting abuse through the measures imposed by governments and service providers (Figure 2). We believe this knowledge can help various stakeholders (including researchers) become more aware of the gaps that need addressing.

Our paper also discusses how technology's characteristics accentuate the challenges of providing assistance to victims of abuse. We also discuss challenges separate from technology's characteristics (e.g., the inability to determine consent from given evidence), challenges we anticipate might be easier to solve in the short term. The rest of the challenges do not appear insurmountable or as hurdles to be avoided; instead, they appear as pain points that the industry and academia can work on addressing. We view the identified gaps as a call for action in assisting victims, as well as restricting perpetrators and holding them accountable.

Here we discuss possible solutions and research directions for addressing these challenges (summarized in Table I). It should be noted that proper evaluation of the discussed solutions is subject to future research.

C. Investigating abuse (evidence)

The search for digital evidence is often the first step in investigating sexual abuse [155]. However, many challenges exist in collating and using digital evidence in the court of law (§V-A1). We suggest possible solutions and research directions for addressing the challenges of investigating abuse and using its evidence.

*1) **Evolution and opaqueness**:* Stakeholders and victims need to understand technologies enough to avoid dangerous errors (see §V-A1 and [183]). This is where the research community could help with developing strategies to make technology less opaque. Such improvements could help bridge the knowledge gap, reduce misconceptions, increase trust in the technology, and facilitate the collection of less ambiguous evidence. Betzing et al. [184], for instance, discovered that increasing transparency helped improve comprehension of data practices and policies among the users of mobile devices. Transparency could be achieved by making the devices more intuitive to use [185].

Improving mental models could help victims and stakeholders better understand how they can collate and use evidence. Even before interacting with new technologies, stakeholders implicitly have the notion that new technologies are difficult to use and come with added complexities (§V-A1). However, this perception is not always true. One of the main goals of the usable privacy and security community is to improve users' mental models related to security and privacy aspects of technology [186]. For instance, a research group at Carnegie Mellon University has proposed labels to improve consumers' mental models of IoT devices' security and privacy characteristics [187]. Similarly, the research community could investigate improvements to the mental models of stakeholders to help them make informed decisions about digital evidence.

*2) **Malleability**:* Research in computer forensics could help prove the validity of evidence. Technology is malleable, and it is difficult to prove that a piece of digital evidence has not been tampered with (§V-A1). The possibility of tampered evidence complicates the use of digital evidence in court proceedings ([155], [188].

More research could also be done to improve effectiveness and efficiency when determining the validity of evidence (§V-A1. The advances will be important in collecting and preserving evidence that is tamperproof and admissible in court, while also advancing the justice process more quickly

Category of assistance to victims	Challenges	Possible solutions and research directions
Investigating abuse	Evolution, opaqueness	a. Make solutions intuitive to use. b. Develop features that help improve stakeholders' mental models.
	Malleability	Improve processes and timelines for validating the authenticity of the evidence.
	Reproducibility	Develop features to notify people of content about them being screenshotted or redistributed.
	Consent issues	Develop educational technology campaigns that clarify consent issues.
Reporting and preventing abuse	Covertness, anonymity, publicness, indispensability	a. Develop perpetrator-focused technological solutions that help the perpetrator take responsibility for their actions. b. Service providers could ensure that solutions have high security and privacy for victims.
	Lack of alternative reporting paths	a. Implement anonymous whistleblowing and digital activism. b. Explore alternative reporting paths via the research community.
	Lack of usability, personalization, risk assessment, evaluation, and maintenance	a. Research alternative revenue models for solutions that victims will use. b. Involve stakeholders in establishing unison and developing solutions.
Restricting abuse	Different legislative laws across jurisdictions	Make legislative laws more uniform across states.
	Lack of adequate involvement from solution providers to make technology safer	a. Involve social media service providers in making the default setting a more private and restricted option. b. Use the various characteristics of technologies as a model when service providers are brainstorming how their solutions can be misused. Providers should incorporate safety by design in their products.

TABLE I: Possible solutions and research directions

for victims [189]. At the same time, such research could help an accused demonstrate that sexual abuse, in fact, did not happen either because there was consent or because there was no action by the accused that can be interpreted as sexual abuse.

3) ***Reproducibility****:* Many characteristics worsen the impact of revictimization for victims. As seen in §V-A1, the duplication and redistribution of the victim's sexual content without consent violates the victim's privacy. Because reproducibility is an inherent characteristic of technology, it may be difficult to address this challenge in the short term. Duplicated sexual content could constitute pornography, and various ongoing research is focused on reducing the speed of redistribution of pornographic content [190]. To improve victims' privacy and help them have more control over their online sexual content, future research, for instance, could look into methods of notifying people about redistributed digital content that includes them.

4) ***Issues of consent****:* In gathering evidence, victims lack clarity on whether consent is needed to record the other party sexually abusing them. Victims put their safety and lives at risk without knowing if the recordings obtained without consent will be accepted in court (§V-A1). We suggest the government clarifies the state's position on this [191]. For instance, educational campaigns have been developed that explain what constitutes consent in carrying out sexual activities [192]. Such campaigns could also clarify exceptions to obtaining consent prior to victims recording their sexual abuse incident.

In investigating gathered evidence, it is also difficult to determine if consent was given to engage in sexual activity. It is even harder to determine if consent was initially given and later revoked (§V-A1). While there are technological solutions proposed to capture both parties' consent before the start of a sexual activity [193], they fail to capture revoked consent [194]. Even though future research in technology can look into capturing consent for the whole duration of sexual activity, this may be a challenge beyond the scope of technology. Other approaches may need to be explored in combination with technology.

D. Reporting and preventing abuse (technological solutions)

We discuss how the characteristics of technology facilitate the challenges of using technological solutions. We also discuss other challenges that are not linked to technological characteristics and possible solutions to these challenges.

1) ***Multiple technological characteristics****:* Stakeholders put the burden on the victim to stay safe by altering their use of technology. This action supports victim blaming (see §V-B1). Also, asking the victim to alter their use of technologies is almost impossible due to its indispensability [39]. The concept of digital minimalism [195], for instance, illustrates how difficult it is for people to do away with technology. The research community could investigate ways of avoiding surveillance without victims minimizing their use of technology.

Further, some characteristics of technology contribute to security and privacy concerns around using solutions (see Section IV). Because of the sensitive information that such solutions would hold, solution providers should consider those that provide high security and privacy for victims. Further, solution providers should effectively communicate to victims about their solutions' security and privacy to reduce information asymmetry.

2) ***Anonymity****:* Rather than visit a police station in person, technological reporting solutions could help people report sexual abuse incidents from the privacy of their homes [196]. Some stakeholders, however, fear an increase in false reporting due to the anonymity that technological solutions provide (§V-B1). While this is a valid concern, compared to the staggering findings that 95% of victims do not report being sexually abused [197], addressing the assumption of false reporting may currently be the wrong problem to address.

3) ***Alternative reporting paths****:* Most solutions provide victims with one path to reporting with no alternatives, which is rigid and problematic (e.g., when someone in a high ranking position, such as a law enforcement agent or a support worker, is the perpetrator). The information security principle Defence in Depth calls for avoiding a single point of failure [183]. Solutions should be designed to have other paths for reporting should one "fail."

The research community could explore other pathways by which victims can pursue justice. Digital activism, for example, could be helpful in this regard; however, it has been known to lead to revictimization [153]. Anonymous whistleblowing could also help victims bypass an organization's formal reporting structure and notify the authorities or upper management. Liu [157] described a whistleblowing solution implemented in the form of a Google spreadsheet that listed people who have abused others in the media industry. This spreadsheet was circulated among individuals in the industry to inform

others and add more names to the list. The solution, however, faced three main problems: (i) it was not anonymous since people could determine the originator of the list; (ii) people were afraid of false reporting, which could immediately tarnish the images of others; and (iii) such an approach did not help the victims in their pursuit of justice. These are three main challenges in using whistleblowing alternatives to reporting that future research could address.

*4) **More effective technological solutions**:* Solutions have low usability and lack personalization, risk assessment, evaluation, and maintenance. Victims also do not know where to find solutions or that certain solutions exist (§V-B1). We discovered two major reasons for the above issues: the lack of appropriate revenue models and the failure to involve stakeholders in solution development.

The revenue model for developing solutions for victims needs to be rethought. Our results suggest victims found apps that charged fees exploitative and were unwilling to pay for them (§V-B1). It seems improper to charge someone in distress to use technological solutions. However, the information market is characterized by huge upfront investments in technology design, though the marginal costs of scaling are almost negligible [198], [198]. Typically, companies recover this money through a number of revenue models such as subscription services, advertising, freemium models, etc [199]. However, these revenue models do not seem to work for solutions assisting the targets of sexual abuse (§V-B1). For example, a subscription service would seem inappropriate, asking people to pay subscription fees pending a time they get abused and can then use the solution to get justice. Currently, the most optimal way to get resources to develop solutions is to apply for funding from the government or other organizations [200]. However, the usage of this funding may be restricted to certain conditions that guide the organization [200]. For more effective technological solutions to be developed and maintained, research is needed for a revenue model where the developer makes money to sustain and maintain the product while the victims do not feel exploited.

Further, all stakeholders need to be in unison and be involved in developing solutions. Our results show that the development of solutions in isolation is problematic (§V-B1). Stakeholders need to be on board for the technological solutions to be trauma informed, effective, and not result in more harm than good for victims [43].

E. Restricting abuse (government and service providers)

*1) **Uniform legislative laws**:* Laws vary across jurisdictions, making it hard to hold perpetrators accountable. The *boundlessness* of technology makes it possible for perpetrators to meet people in various jurisdictions, commit sex crimes, and return to their jurisdictions (§V-C1). For instance, one of the most notorious serial rapists and murderers in Canada, Paul Bernardo, was based in St. Catharines, ON, but was abusing victims in Hamilton, ON. Contradictions in jurisdiction laws in both cities made it harder to apprehend him [201]. Though Bernardo's situation was not technology facilitated, technology opens up many more avenues for such abuse and presents difficulties with arresting perpetrators. Researchers call for more cohesive legislative laws, at least within countries [62], [138]. Governments could consider such changes to facilitate support for victims.

*2) **Increased service provider involvement**:* To shift the responsibility of staying safe away from victims, service providers need to get more involved and make technology safer for victims to use (§V-C1). Some principles of designing secure systems could be used as guidelines to help service providers build better technologies that could reduce abuse for victims. For instance, the Principle of Fail-Safe Defaults states systems should be designed to be "fail-safe, meaning that they fail 'closed' (denying access) rather than 'open' " [183]. This principle implies the default setting for any secured product should be the safe option. For example, social media service providers could consider making the default setting the more private, restrictive option, whereby people cannot tag others or post on other people's social media walls or pages unless the subject enables the setting. This setup could help reduce the amount of public information a perpetrator can find about a victim.

Furthermore, in designing technologies service providers could consider ways in which those technologies can be misused by perpetrators and try to minimize that misuse. Both Kadri and Uusitalo propose this approach to designing everyday technologies and termed the approach *empathy by design* [202] or *safety by design* [174]. While such technological design may be unable to avoid every abuse use case, it could go a long way in providing safer technological solutions than currently exist.

VII. Conclusion

Our research offers the first SoK on technology's dual nature in sexual abuse. We identify characteristics of technology that facilitate abuse and report the challenges in providing support for victims. Our findings suggest the governments, stakeholders, technological service providers, and the research community have a role in reducing abuse and supporting victims of sexual abuse. Without active intervention, developed solutions could result in more harm than help for victims. As society's reliance on technology increases, the need to address the challenges of identifying, preventing, restricting, and reporting abuse grows.

VIII. Acknowledgements

This research has been supported by the funding from Vesta Social Innovation Technologies Inc., Mitacs Accelerate program, and a gift from Scotiabank to UBC. We would like to thank members of the Laboratory for Education and Research in Secure Systems Engineering (LERSSE) who provided their feedback on the reported research. Our anonymous reviewers and shepherd provided important feedback and suggestions to improve the paper. Stylistic and copy editing by Patricia Tomaszewski and Lynn Slobogian helped to improve readability of this paper.

References

[1] 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.

[2] 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.

[3] 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*, vol. 29, no. 4, pp. 671–682, 2014.

[4] B. Cybulska, "Sexual assault: Key issues," *Journal of the Royal Society of Medicine*, vol. 100, no. 7, pp. 321–324, 2007.

[5] S. Dyer, "Sexual assault reports on the rise during pandemic: Sace," https://edmonton.ctvnews.ca/sexual-assault-reports-on-the-rise-during-pandemic-sace-1.5106194?, 2020, accessed: 2021-04-15.

[6] J. Pringle, "Ottawa hospital encourages survivors of sexual assault, partner violence to seek er treatment during pandemic," https://ottawa.ctvnews.ca/ottawa-hospital-encourages-survivors-of-sexual-assault-partner-violence-to-seek-er-treatment-during-pandemic-1.4903698, 2020, accessed: 2021-04-15.

[7] J. Suh, E. Horvitz, R. W. White, and T. Althoff, "Population-scale study of human needs during the covid-19 pandemic: Analysis and implications," in *Proceedings of the 14th ACM International Conference on Web Search and Data Mining*, 2021, pp. 4–12.

[8] T. Barrow, "Sexual assault centre's crisis calls on the rise during pandemic," https://calgary.ctvnews.ca/sexual-assault-centre-s-crisis-calls-on-the-rise-during-pandemic-1.5119438, 2020, accessed: 2021-04-15.

[9] SACE, "Sace services during covid-19," https://www.sace.ca/covid-19/, 2020, accessed: 2021-04-15.

[10] K. Usher, N. Bhullar, J. Durkin, N. Gyamfi, and D. Jackson, "Family violence and covid-19: Increased vulnerability and reduced options for support," *International journal of mental health nursing*, 2020.

[11] U. Women, "The shadow pandemic: Violence against women during covid-19," https://www.unwomen.org/en/news/in-focus/in-focus-gender-equality-in-covid-19-response/violence-against-women-during-covid-19, 2021, accessed: 2021-08-20.

[12] F. Al Mamun, I. Hosen, and M. A. Mamun, "Sexual violence and rapes' increment during the covid-19 pandemic in bangladesh," *EClinicalMedicine*, vol. 34, 2021.

[13] N. Henry and A. Powell, "Embodied harms: Gender, shame, and technology-facilitated sexual violence," *Violence against women*, vol. 21, no. 6, pp. 758–779, 2015.

[14] J. F. Wolfswinkel, E. Furtmueller, and C. P. Wilderom, "Using grounded theory as a method for rigorously reviewing literature," *European journal of information systems*, vol. 22, no. 1, pp. 45–55, 2013.

[15] 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.

[16] M. Webster, "Sexual assault," https://www.merriam-webster.com/dictionary/rape, 2021, accessed: 2021-04-12.

[17] Lexico, "Perpetrator," https://www.lexico.com/definition/perpetrator, 2021, accessed: 2021-04-12.

[18] E. Mencarini, A. Rapp, L. Tirabeni, and M. Zancanaro, "Designing wearable systems for sports: A review of trends and opportunities in human–computer interaction," *IEEE Transactions on Human-Machine Systems*, vol. 49, no. 4, pp. 314–325, 2019.

[19] J. Nicolás, J. M. C. De Gea, B. Nicolas, J. L. Fernandez-Aleman, and A. Toval, "On the risks and safeguards for requirements engineering in global software development: Systematic literature review and quantitative assessment," *IEEE Access*, vol. 6, pp. 59 628–59 656, 2018.

[20] Z. S. H. Abad, M. Noaeen, and G. Ruhe, "Requirements engineering visualization: a systematic literature review," in *2016 IEEE 24th International Requirements Engineering Conference (RE)*. IEEE, 2016, pp. 6–15.

[21] I. Homoliak, F. Toffalini, J. Guarnizo, Y. Elovici, and M. Ochoa, "Insight into insiders and it: A survey of insider threat taxonomies, analysis, modeling, and countermeasures," *ACM Computing Surveys (CSUR)*, vol. 52, no. 2, pp. 1–40, 2019.

[22] A. Ayobi, P. Marshall, and A. L. Cox, "Reflections on 5 years of personal informatics: rising concerns and emerging directions," in *Proceedings of the 2016 CHI conference extended abstracts on human factors in computing systems*, 2016, pp. 2774–2781.

[23] E. A. Ruvalcaba-Gomez, J. I. Criado, and J. R. Gil-Garcia, "Discussing open government as a concept: a comparison between the perceptions of public managers and current academic debate," in *Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age*, 2018, pp. 1–10.

[24] A.-W. Harzing, *The publish or perish book*. Tarma Software Research Pty Limited Melbourne, Australia, 2010.

[25] Taster. (2019) Google scholar, web of science, and scopus: Which is best for me? [Online]. Available: https://blogs.lse.ac.uk/impactofsocialsciences/2019/12/03/google-scholar-web-of-science-and-scopus-which-is-best-for-me/

[26] C. J. Pannucci and E. G. Wilkins, "Identifying and avoiding bias in research," *Plastic and reconstructive surgery*, vol. 126, no. 2, p. 619, 2010.

[27] H. Noble and J. Smith, "Issues of validity and reliability in qualitative research," *Evidence-based nursing*, vol. 18, no. 2, pp. 34–35, 2015.

[28] P. Forde and A. Patterson, *Paedophile internet activity*. Australian Institute of Criminology Canberra, 1998.

[29] D. Turner. (March 12, 2020) Should you use inter-rater reliability in qualitative coding? [Online]. Available: https://www.quirkos.com/blog/post/inter-rater-reliaiblity-qualitative-coding-data/

[30] I. Lopez-Neira, T. Patel, S. Parkin, G. Danezis, and L. Tanczer, "'internet of things': How abuse is getting smarter," 2019.

[31] C. Snook, "Safelives," *Tech vs abuse: research findings*, 2017.

[32] 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*, 2017, pp. 2189–2201.

[33] 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)*, 2019, pp. 105–122.

[34] 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*, vol. 24, no. 1, pp. 53–59, 2009.

[35] 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)*. IEEE, 2018, pp. 441–458.

[36] 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*, vol. 33, no. 4, pp. 135–150, 2015.

[37] 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.

[38] 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.

[39] C. L. Mason and S. Magnet, "Surveillance studies and violence against women," *surveillance & society*, vol. 10, no. 2, pp. 105–118, 2012.

[40] H. Douglas, B. A. Harris, and M. Dragiewicz, "Technology-facilitated domestic and family violence: Women's experiences," *The British Journal of Criminology*, vol. 59, no. 3, pp. 551–570, 2019.

[41] C. B. Draucker and D. S. Martsolf, "The role of electronic communication technology in adolescent dating violence," *Journal of Child and Adolescent Psychiatric Nursing*, vol. 23, no. 3, pp. 133–142, 2010.

[42] N. Henry and A. Powell, "The dark side of the virtual world," in *Preventing Sexual Violence*. Springer, 2014, pp. 84–104.

[43] 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*, vol. 33, no. 2, pp. 133–155, 2015.

[44] E. Borrajo, M. Gámez-Guadix, and E. Calvete, "Cyber dating abuse: Prevalence, context, and relationship with offline dating aggression," *Psychological reports*, vol. 116, no. 2, pp. 565–585, 2015.

[45] 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*, vol. 30, no. 3, pp. 381–392, 2015.

[46] 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)*, 2020, pp. 1893–1909.

[47] R. Gillett, "Intimate intrusions online: Studying the normalisation of abuse in dating apps," in *Women's Studies International Forum*, vol. 69. Elsevier, 2018, pp. 212–219.

[48] N. Ramsay, V. Carr, L. Sailer, M. McDermott, S. Shenai, and D. A. Yassien, "Tech vs abuse: Research findings," 2019.

[49] 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*, vol. 36, no. 6, pp. 430–438, 2015.

[50] J. A. Dunlap, "Intimate terrorism and technology: There's and app for that," *U. Mass. L. Rev.*, vol. 7, p. 10, 2012.

[51] 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.

[52] 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*, 2018, pp. 1–6.

[53] B. A. Harris and D. Woodlock, "Digital coercive control: Insights from two landmark domestic violence studies," *The British Journal of Criminology*, vol. 59, no. 3, pp. 530–550, 2019.

[54] 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*, vol. 40, no. 11, pp. 1170–1196, 2019.

[55] 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*, 2018, pp. 1–13.

[56] L. F. Cardoso, S. B. Sorenson, O. Webb, and S. Landers, "Recent and emerging technologies: Implications for women's safety," *Technology in Society*, vol. 58, p. 101108, 2019.

[57] K. Duerksen, "Technological intimate partner violence: victim impacts and technological perpetration factors," Ph.D. dissertation, 2018.

[58] R. Leitão, "Technology-facilitated intimate partner abuse: a qualitative analysis of data from online domestic abuse forums," *Human–Computer Interaction*, pp. 1–40, 2019.

[59] 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)*. IEEE, 2020, pp. 626–643.

[60] A. Attrill-Smith and C. Wesson, "The psychology of cybercrime," *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, pp. 653–678, 2020.

[61] 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*, pp. 1–24, 2019.

[62] 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*, pp. 1–12, 2020.

[63] B. A. Harris, "Technology and violence against women," in *The Emerald Handbook of Feminism, Criminology and Social Change*. Emerald Publishing Limited, 2020.

[64] 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*, vol. 29, no. 3-4, 2020.

[65] 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.

[66] V. Greiman and C. Bain, "The emergence of cyber activity as a gateway to human trafficking," *Journal of Information Warfare*, vol. 12, no. 2, pp. 41–49, 2013.

[67] 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*, vol. 19, no. 4, pp. 390–417, 2014.

[68] A. van Moorsel, M. Emms, G. Rendall, and B. Arief, "Digital strategy for the social inclusion of survivors of domestic violence," 2011.

[69] 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.

[70] J. M. Blythe and S. D. Johnson, "A systematic review of crime facilitated by the consumer internet of things," *Security Journal*, pp. 1–29, 2019.

[71] D. Chen, S. Kalra, D. Irwin, P. Shenoy, and J. Albrecht, "Preventing occupancy detection from smart meters," *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2426–2434, 2015.

[72] T. Reichherzer, M. Timm, N. Earley, N. Reyes, and V. Kumar, "Using machine learning techniques to track individuals & their fitness activities," in *CATA 2017*. ISCA, 2017, pp. 119–124.

[73] 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)*. IEEE, 2015, pp. 1–7.

[74] 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*, 2019, pp. 527–539.

[75] 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*, 2019, pp. 1–15.

[76] L. Tanczer, S. Parkin, T. Patel, I. Lopez-Neira, and J. Slupska, "Ucl's gender and internet of things (iot) research project," 2019.

[77] 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*, vol. 61, no. 4, pp. 39–55, 2010.

[78] 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*, vol. 32, no. 2, pp. 205–217, 2016.

[79] 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*, vol. 1, no. CSCW, pp. 1–22, 2017.

[80] A. Powell and N. Henry, *Sexual violence in a digital age*. Springer, 2017.

[81] R. Gillett, "Intimate intrusions online: Studying the normalisation of abuse in dating apps," in *Women's Studies International Forum*, vol. 69. Elsevier, 2018, pp. 212–219.

[82] D. Woodlock, "The abuse of technology in domestic violence and stalking," *Violence against women*, vol. 23, no. 5, pp. 584–602, 2017.

[83] 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)*, 2019, pp. 105–122.

[84] B. A. Harris and D. Woodlock, "Digital coercive control: Insights from two landmark domestic violence studies," *The British Journal of Criminology*, vol. 59, no. 3, pp. 530–550, 2019.

[85] 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," Ph.D. dissertation, University of Missouri–Columbia, 2013.

[86] A. Powell and N. Henry, "Policing technology-facilitated sexual violence against adult victims: Police and service sector perspectives," *Policing and Society*, vol. 28, no. 3, pp. 291–307, 2018.

[87] A. Powell, "Configuring consent: Emerging technologies, unauthorized sexual images and sexual assault," *Australian & New Zealand journal of criminology*, vol. 43, no. 1, pp. 76–90, 2010.

[88] 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*, vol. 18, no. 4, pp. 609–625, 2018.

[89] 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*, 2019, pp. 1–14.

[90] L. Vitis, M. A. Joseph, and M. D. Mahadevan, "Technology and sexual violence: Sacc summary report," 2017.

[91] 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*, vol. 20, no. 2, pp. 25–29, 2013.

[92] 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*, vol. 47, no. 2, pp. 183–190, 2010.

[93] J. P. Dimond, C. Fiesler, and A. S. Bruckman, "Domestic violence and information communication technologies," *Interacting with computers*, vol. 23, no. 5, pp. 413–421, 2011.

[94] J. A. Kloess, A. R. Beech, and L. Harkins, "Online child sexual exploitation: Prevalence, process, and offender characteristics," *Trauma, Violence, & Abuse*, vol. 15, no. 2, pp. 126–139, 2014.

[95] Facebook, "Using facebook-tagging," https://www.facebook.com/help/tagging, 2021, accessed: 2021-03-30.

[96] E. Quayle and M. Taylor, "Child seduction and self-representation on the internet," *CyberPsychology & Behavior*, vol. 4, no. 5, pp. 597–608, 2001.

[97] A. A. Gillespie, "Child protection on the internet-challenges for criminal law," *Child & Fam. LQ*, vol. 14, p. 411, 2002.

[98] 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*, pp. 1–24, 2019.

[99] T. Project, "About the tor project," https://www.torproject.org, 2021, accessed: 2021-04-15.

[100] R. Cohen-Almagor, "Online child sex offenders: Challenges and counter-measures," *The Howard Journal of Criminal Justice*, vol. 52, no. 2, pp. 190–215, 2013.

[101] 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*, vol. 47, no. 2, pp. 183–190, 2010.

[102] 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*. Citeseer, 2010, pp. 1–17.

[103] K. McCartan and R. McAlister, "Mobile phone technology and sexual abuse," *Information & Communications Technology Law*, vol. 21, no. 3, pp. 257–268, 2012.

[104] D. Zinoviev and V. Duong, "Toward understanding friendship in online social networks," *arXiv preprint arXiv:0902.4658*, 2009.

[105] J. Bryce, "Online sexual exploitation of children and young people," *Handbook of internet crime*, pp. 320–342, 2010.

[106] D. K. Citron, *Hate crimes in cyberspace*. Harvard University Press, 2014.

[107] M. J. Scannell, "Online dating and the risk of sexual assault to college students," *Building Healthy Academic Communities Journal*, vol. 3, no. 1, pp. 34–43, 2019.

[108] C. Cross, M. Dragiewicz, and K. Richards, "Understanding romance fraud: Insights from domestic violence research," *The British Journal of Criminology*, vol. 58, no. 6, pp. 1303–1322, 2018.

[109] 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*, vol. 23, no. 1, pp. 43–71, 2011.

[110] T. J. Holt, K. R. Blevins, and N. Burkert, "Considering the pedophile subculture online," *Sexual Abuse*, vol. 22, no. 1, pp. 3–24, 2010.

[111] B. Orbach and L. Huang, "Con men and their enablers: The anatomy of confidence games," *Social Research: An International Quarterly*, vol. 85, no. 4, pp. 795–822, 2018.

[112] M. A. Henderson, *Flimflam Man: How Con Games Work*. Paladin Press, 1985.

[113] M. C. Taylor, *Confidence games: Money and markets in a world without redemption*. University of Chicago Press, 2004.

[114] R. J. Heintzman, "Confidence schemes and con games: Old games with new players," *FBI L. Enforcement Bull.*, vol. 55, p. 11, 1986.

[115] 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*, vol. 23, no. 1, pp. 43–71, 2011.

[116] M. A. Pendergrass, "The intersection of human trafficking and technology," Ph.D. dissertation, Utica College, 2018.

[117] K. J. Mitchell and d. boyd, "Understanding the role of technology in the commercial sexual exploitation of children: the perspective of law enforcement." 2014.

[118] 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*, 2014, pp. 201–204.

[119] D. M. Hughes, "Trafficking in human beings in the european union: Gender, sexual exploitation, and digital communication technologies," *Sage Open*, vol. 4, no. 4, p. 2158244014553585, 2014.

[120] E. Quayle and M. Taylor, "Child pornography and the internet: Perpetuating a cycle of abuse," *Deviant behavior*, vol. 23, no. 4, pp. 331–361, 2002.

[121] V. Bouche, "A report on the use of technology to recruit, groom and sell domestic minor sex trafficking victims," 2015.

[122] N. Henry and A. Powell, "Beyond the 'sext': Technology-facilitated sexual violence and harassment against adult women," *Australian & New Zealand Journal of Criminology*, vol. 48, no. 1, pp. 104–118, 2015.

[123] 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*. Australian Institute of Criminology Canberra, 2009, vol. 103.

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

[125] J. Elliott and K. McCartan, "The reality of trafficked people's access to technology," *The Journal of Criminal Law*, vol. 77, no. 3, pp. 255–273, 2013.

[126] R. Pennington and J. Birthisel, "When new media make news: Framing technology and sexual assault in the Steubenville rape case," *New Media & Society*, vol. 18, no. 11, pp. 2435–2451, 2016.

[127] C. McGlynn, E. Rackley, and R. Houghton, "Beyond 'revenge porn': The continuum of image-based sexual abuse," *Feminist Legal Studies*, vol. 25, no. 1, pp. 25–46, 2017.

[128] N. Henry, A. Flynn, and A. Powell, "Policing image-based sexual abuse: Stakeholder perspectives," *Police practice and research*, vol. 19, no. 6, pp. 565–581, 2018.

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

[130] R. M. Hayes and M. Dragiewicz, "Unsolicited dick pics: Erotica, exhibitionism or entitlement?" in *Women's Studies International Forum*, vol. 71. Elsevier, 2018, pp. 114–120.

[131] N. Henry and A. Flynn, "Image-based sexual abuse: A feminist criminological approach," *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, pp. 1109–1130, 2020.

[132] A. Flynn and N. Henry, "Image-based sexual abuse: an australian reflection," *Women & Criminal Justice*, pp. 1–14, 2019.

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

[134] A. Powell and N. Henry, "Technology-facilitated sexual violence victimization: Results from an online survey of australian adults," *Journal of interpersonal violence*, vol. 34, no. 17, pp. 3637–3665, 2019.

[135] 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*, vol. 1, no. 2, p. 3, 2019.

[136] A. Powell, A. Scott, A. Flynn, and N. Henry, "Image-based sexual abuse: An international study of victims and perpetrators," 2020.

[137] A. Dodge, "Digitizing rape culture: Online sexual violence and the power of the digital photograph," *Crime, media, culture*, vol. 12, no. 1, pp. 65–82, 2016.

[138] A. Powell, "Configuring consent: Emerging technologies, unauthorized sexual images and sexual assault," *Australian & New Zealand journal of criminology*, vol. 43, no. 1, pp. 76–90, 2010.

[139] C. Calvert and J. Brown, "Video voyeurism, privacy, and the internet: Exposing peeping toms in cyberspce," *Cardozo Arts & Ent. LJ*, vol. 18, p. 469, 2000.

[140] N. Henry and A. Powell, "Technology-facilitated sexual violence: A literature review of empirical research," *Trauma, violence, & abuse*, vol. 19, no. 2, pp. 195–208, 2018.

[141] A. Flynn and N. Henry, "Image-based sexual abuse: an australian reflection," *Women & Criminal Justice*, pp. 1–14, 2019.

[142] 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*, vol. 92, pp. 393–402, 2019.

[143] 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)*, 2019, pp. 89–104.

[144] A. Powell, "Seeking rape justice: Formal and informal responses to sexual violence through technosocial counter-publics," *Theoretical Criminology*, vol. 19, no. 4, pp. 571–588, 2015.

[145] Twitter, "About twitter," https://about.twitter.com/, 2021, accessed: 2021-04-11.

[146] Facebook, "About facebook," https://about.fb.com, 2021, accessed: 2021-04-11.

[147] Youtube, "About youtube," https://www.youtube.com/about/, 2021, accessed: 2021-04-11.

[148] 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*, vol. 13, no. 5, pp. 477–497, 2018.

[149] A. G. Campbell, *Bernardo investigation review*. Solicitor General and Correctional Services, 1996.

[150] 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*, vol. 47, no. 2, pp. 183–190, 2010.

[151] M. C. Joyce, *Digital activism decoded: The new mechanics of change*. IDEA, 2010.

[152] R. Chowdhury and B. Fileborn, ""break the silence bangladesh": Examining "everyday" experiences of sexual violence through online activism," in *Women's Studies International Forum*, vol. 81. Elsevier, 2020, p. 102379.

[153] S. Sills, C. Pickens, K. Beach, L. Jones, O. Calder-Dawe, P. Benton-Greig, and N. Gavey, "Rape culture and social media: Young critics and a feminist counterpublic," *Feminist Media Studies*, vol. 16, no. 6, pp. 935–951, 2016.

[154] C. B. Draucker and D. S. Martsolf, "Storying childhood sexual abuse," *Qualitative health research*, vol. 18, no. 8, pp. 1034–1048, 2008.

[155] A. Dodge, D. Spencer, R. Ricciardelli, and D. Ballucci, ""this isn't your father's police force": Digital evidence in sexual assault investigations," *Australian & New Zealand Journal of Criminology*, vol. 52, no. 4, pp. 499–515, 2019.

[156] M. Lindsay, J. T. Messing, J. Thaller, A. Baldwin, A. Clough, T. Bloom, K. B. Eden, and N. Glass, "Survivor feedback on a safety decision aid smartphone application for college-age women in abusive relationships," *Journal of Technology in Human Services*, vol. 31, no. 4, pp. 368–388, 2013.

[157] H. Liu, "When whispers enter the cloud: Evaluating technology to prevent and report sexual assault," *Harv. JL & Tech.*, vol. 31, p. 939, 2017.

[158] R. S. Portnoff, D. Y. Huang, P. Doerfler, S. Afroz, and D. McCoy, "Backpage and bitcoin: Uncovering human traffickers," in *Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 2017, pp. 1595–1604.

[159] N. van Gelder, K. van Rosmalen-Nooijens, S. A Ligthart, J. Prins, S. Oertelt-Prigione, and A. Lagro-Janssen, "Safe: an ehealth intervention for women experiencing intimate partner violence–study protocol for a randomized controlled trial, process evaluation and open feasibility study," *BMC public health*, vol. 20, pp. 1–8, 2020.

[160] L. Brignone and J. L. Edleson, "The dating and domestic violence app rubric: synthesizing clinical best practices and digital health app standards for relationship violence prevention smartphone apps," *International Journal of Human–Computer Interaction*, vol. 35, no. 19, pp. 1859–1869, 2019.

[161] S. Sinha, A. Shrivastava, and C. Paradis, "A survey of the mobile phone-based interventions for violence prevention among women," *Advances in Social Work*, vol. 19, no. 2, pp. 493–517, 2019.

[162] K. Hegarty, L. Tarzia, E. Murray, J. Valpied, C. Humphreys, A. Taft, L. Gold, and N. Glass, "Protocol for a randomised controlled trial of a web-based healthy relationship tool and safety decision aid for women experiencing domestic violence (i-decide)," *BMC public health*, vol. 15, no. 1, pp. 1–9, 2015.

[163] N. Glass, A. Clough, J. Case, G. Hanson, J. Barnes-Hoyt, A. Waterbury, J. Alhusen, M. Ehrensaft, K. T. Grace, and N. Perrin, "A safety app to respond to dating violence for college women and their friends: the myplan study randomized controlled trial protocol," *BMC public health*, vol. 15, no. 1, pp. 1–13, 2015.

[164] C. E. Powell, "Project aletheia: A web-based support network for survivors of campus sexual assault," Ph.D. dissertation, Mills College, 2017.

[165] R. Bellini, S. Forrest, N. Westmarland, and J. D. Smeddinck, "Mechanisms of moral responsibility: Rethinking technologies for domestic violence prevention work," in *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 2020, pp. 1–13.

[166] L. Tarzia, R. Cornelio, K. Forsdike, and K. Hegarty, "Women's experiences receiving support online for intimate partner violence: how does it compare to face-to-face support from a health professional?" *Interacting with Computers*, vol. 30, no. 5, pp. 433–443, 2018.

[167] 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*, vol. 24, no. 1, pp. 53–59, 2009.

[168] I. Rodríguez-Rodríguez, J.-V. Rodríguez, A. Elizondo-Moreno, P. Heras-González, and M. Gentili, "Towards a holistic ICT platform for protecting intimate partner violence survivors based on the iot paradigm," *Symmetry*, vol. 12, no. 1, p. 37, 2020.

[169] N. Glass, K. B. Eden, T. Bloom, and N. Perrin, "Computerized aid improves safety decision process for survivors of intimate partner violence," *Journal of interpersonal violence*, vol. 25, no. 11, pp. 1947–1964, 2010.

[170] R. Fiolet, L. Tarzia, R. Owen, C. Eccles, K. Nicholson, M. Owen, S. Fry, J. Knox, and K. Hegarty, "Indigenous perspectives on using technology as a supportive resource when experiencing family violence," *Journal of Technology in Human Services*, vol. 38, no. 3, pp. 203–225, 2020.

[171] M. Ford-Gilboe, C. Varcoe, K. Scott-Storey, J. Wuest, J. Case, L. M. Currie, N. Glass, M. Hodgins, H. MacMillan, N. Perrin *et al.*, "A tailored online safety and health intervention for women experiencing intimate partner violence: the ican plan 4 safety randomized controlled trial protocol," *BMC Public Health*, vol. 17, no. 1, pp. 1–12, 2017.

[172] V. Neelam, "Mobile application for survivors of domestic violence," 2018.

[173] M. N. Islam, N. T. Promi, J. M. Shaila, M. A. Toma, M. A. Pushpo, F. B. Alam, S. N. Khaledur, T. T. Anannya, and M. F. Rabbi, "Safeband: A wearable device for the safety of women in bangladesh," in *Proceedings of the 16th International Conference on Advances in Mobile Computing and Multimedia*, 2018, pp. 76–83.

[174] L. Uusitalo, "Designing for women experiencing intimate partner violence," 2018.

[175] S. L. Martin, J. McLean, C. Brooks, and K. Wood, ""i've been silenced for so long": Relational engagement and empowerment in a digital storytelling project with young women exposed to dating violence," *International Journal of Qualitative Methods*, vol. 18, p. 1609406919825932, 2019.

[176] J. A. Blayney, T. Jenzer, J. P. Read, J. A. Livingston, and M. Testa, "Enlisting friends to reduce sexual victimization risk: There's an app for that… but nobody uses it," *Journal of American college health*, vol. 66, no. 8, pp. 767–773, 2018.

[177] C. Southworth and S. Tucker, "Technology, stalking and domestic violence victims," *Miss. LJ*, vol. 76, p. 667, 2006.

[178] L. Tarzia, D. Iyer, E. Thrower, and K. Hegarty, ""technology doesn't judge you": Young australian women's views on using the internet and smartphones to address intimate partner violence," *Journal of technology in human services*, vol. 35, no. 3, pp. 199–218, 2017.

[179] N. E. Glass, N. A. Perrin, G. C. Hanson, T. L. Bloom, J. T. Messing, A. S. Clough, J. C. Campbell, A. C. Gielen, J. Case, and K. B. Eden, "The longitudinal impact of an internet safety decision aid for abused women," *American journal of preventive medicine*, vol. 52, no. 5, pp. 606–615, 2017.

[180] R. Bellini, A. Strohmayer, P. Olivier, and C. Crivellaro, "Mapping the margins: Navigating the ecologies of domestic violence service provision," in *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 2019, pp. 1–13.

[181] B. Obada-Obieh, L. Spagnolo, and K. Beznosov, "Towards understanding privacy and trust in online reporting of sexual assault," in *Sixteenth Symposium on Usable Privacy and Security ({SOUPS} 2020)*, 2020, pp. 145–164.
[182] D. Dodd-McCue and A. Tartaglia, "Self-report response bias: Learning how to live with its diagnosis in chaplaincy research," *Chaplaincy Today*, vol. 26, no. 1, pp. 2–8, 2010.
[183] P. C. van Oorschot, *Computer Security and the Internet*. Springer, 2020.
[184] J. H. Betzing, M. Tietz, J. vom Brocke, and J. Becker, "The impact of transparency on mobile privacy decision making," *Electronic Markets*, vol. 30, no. 3, pp. 607–625, 2020.
[185] I. D. Foundation, "Intuitive design," https://www.interaction-design.org/literature/topics/intuitive-design, 2021, accessed: 2021-04-14.
[186] 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*, 2009, pp. 1–12.
[187] C. M. University, "Iot security & privacy label," https://www.iotsecurityprivacy.org, 2021, accessed: 2021-04-14.
[188] J. Cosic, Z. Cosic, J. Ćosić, and Z. Ćosić, "Chain of custody and life cycle of digital evidence," *Computer Technology and Aplications*, vol. 3, pp. 126–129, 2012.
[189] Y. Prayudi and A. Sn, "Digital chain of custody: State of the art," *International Journal of Computer Applications*, vol. 114, no. 5, 2015.
[190] J. V. Eggestein and K. J. Knapp, "Fighting child pornography: A review of legal and technological developments," *Journal of Digital Forensics, Security and Law*, vol. 9, no. 4, p. 3, 2014.
[191] P. C. Lawyers, "Is it a crime to videotape your sexual encounter with someone without his or her consent?" https://www.torontodefencelawyers.com/blog/is-it-a-crime-to/crime-videotape-sexual-encounter-someone-without-consent/, 2021, accessed: 2021-04-14.
[192] C. Women, "Sexual consent campaign," https://www.womens.cusu.cam.ac.uk/campaigns/consent/, 2021, accessed: 2021-04-14.
[193] L. Fling, "Get explicit about sexual consent," https://legalfling.io/#iq-home, 2021, accessed: 2021-04-14.
[194] M. Salam, "Consent in the digital age: Can apps solve a very human problem?" https://www.nytimes.com/2018/03/02/technology/consent-apps.html, 2021, accessed: 2021-04-14.
[195] K. Kowalski, "Digital minimalism defined & 10 digital declutter tips," https://www.sloww.co/digital-minimalism/, 2021, accessed: 2021-03-31.
[196] VESTA, "Vesta social innovation technologies," https://www.vestasit.com, 2020, accessed: 2021-04-14.
[197] S. Perreault, "Criminal victimization in canada, 2014," *Juristat*, vol. 35, no. 1, pp. 1–43, 2015.
[198] M. Hutter, "Information goods," in *Handbook of Cultural Economics, Third Edition*. Edward Elgar Publishing, 2020.
[199] A. Kumar, "The ultimate master list of revenue models used by web and mobile companies," https://yourstory.com/2014/03/ultimate-master-list-revenue-models-web-mobile-companies?utm_pageloadtype=scroll, 2020, accessed: 2021-04-14.
[200] K. Sebelius, "Announcing the winners of the apps against abuse technology challenge," https://obamawhitehouse.archives.gov/blog/2011/11/01/announcing-winners-apps-against-abuse-technology-challenge, 2011, accessed: 2021-04-15.
[201] J. Keller, "Pickton investigation plagued by same issues that failed to stop bernardo," https://www.theglobeandmail.com/news/british-columbia/pickton-investigation-plagued-by-same-issues-that-failed-to-stop-bernardo/article4170926/, 2021, accessed: 2021-03-31.
[202] T. E. Kadri, "Networks of empathy," *Utah L. Rev.*, p. 1075, 2020.
[203] B. Eterovic-Soric, K.-K. R. Choo, H. Ashman, and S. Mubarak, "Stalking the stalkers–detecting and deterring stalking behaviours using technology: A review," *Computers & security*, vol. 70, pp. 278–289, 2017.
[204] K. E. Levy, "Intimate surveillance," *Idaho L. Rev.*, vol. 51, p. 679, 2014.

APPENDIX A
CODEBOOK

The tables in this appendix show various sub-themes that emerged during our coding process. We grouped and renamed similar subthemes. The grouped themes are presented in Sections IV & V.

Theme	Subthemes	Definitions	Examples
1. How technology facilitates sexual abuse	The anonymity 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" [123].
	The malleability 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" [203].
	Lack of well-defined boundaries	No physical limit to the perpetrator's reach	"Participants felt that the fluidity between online and off-line 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 off-line domains" [91].
	Networking	Perpetrators using technology to network with other perpetrators and form stronger bonds	"The Internet may make it easier for CSEC (Cybersecurity) offenders to make connections with other offenders, for example, networking among pimps" [115].
	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" [77].
	The friends 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 befriending the young person, and encouraging them to discuss their life in order to initiate friendship" [105].
	The opaqueness of technology	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" [51].
	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 behavior is that initial and continued engagement is more likely in circumstances where the perpetrator is able to misrepresent themselves as a desirable entity" [91].
	The ever-changing nature of technology	Perpetrators using the evolving nature of technology against victims	"Offenders can use technology to adapt their offending behavior. Consequentially, the constant and continual evolution in technology has ramifications with regard to the facilitation of child sexual abuse and the impact that they have on the prevention of child sexual abuse" [103].

	Distribution of unauthorised materials	The use of technology for the distribution of unauthorized sexual images where sexual abuse 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 abuse, but rather emphasises the continued abuse on the victim where an image is recorded and distributed" [138].
	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" [77].
	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" [148].
	Initiating meetings between the perpetrator and the victim	The use of technology to initiate a 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 abused, and multiple perpetrators may be involved" [91].
	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 virtually" [50].
	Misuse of legitimate tools	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 others" [55].

TABLE A.1: Definitions and examples of sub-themes in our codebook on the theme of how technology facilitates sexual abuse.

Theme	Subthemes	Definitions	Examples
2. How technology assists victims Technological solutions	Technological solutions	The use of technological solutions to prevent and/or report sexual abuse	"The 'SafeBand' system is comprised of a wearable band to be used by the victim, and two mobile applications to be used by the victim and by the police. Women can wear the device as a wristband or locket which will comprise of a button and a light. When the user (victim) presses the button, it identifies the location of the user through Global Positioning System (GPS) and sends a message incorporating the location to the nearest police station and previously saved contacts (number of relatives)" [173].
Challenges with technological solutions	Difficulty in finding solutions	Victims find it difficult to locate the technological solutions	"Many apps studied were difficult to find in the App Store. This limits their visibility and utility to prospective users" [160].
	Lack of complex technical knowledge	Victims need complex technical skill to use technology measures	"One of the major challenges that survivors face is that it requires more effort and more technical knowledge for them to erase their electronic footprints, than it does for their abuser to follow them. Therefore redressing the balance in favour of the survivor will require a range of measures including redesigned websites, history cleaning technologies and training" [68].
	One reporting path	Solutions provide one path of reporting (e.g., when reporting in a university and the offender is a professor)	"There is a need to protect victims from abusers who may have access to victim information because of their jobs. As one participant said, 'Sometimes the abuser is a policeman' " [43].
	Revictimization	Using technology solutions can lead to revictimization	"Despite the potential for a website or app ... to improve access to help and support, the young women emphasized the importance of the technology being safe ... for users. Concerns were raised by some participants over the possibility of a perpetrator or another party viewing a woman's browser history or recently used apps" [178].
	Accessibility issues	Solutions are not accessible	"Accessibility for clients and service providers with disabilities was a concern, especially with already limited financial resources that typically are available to these agencies" [43].
	Facilitating further abuse from perpetrators	The use of technology could facilitate further abuse	"The research shows that survivors have ... barriers to successfully accessing the support services that they require ... the fear of provoking further abuse if their abuser discovers that they have been seeking help" [68].
	Lack of diversity	Solutions have a narrow scope or focus	"Many apps were limited in their scope, providing intervention materials to only a narrow group of users (usually female individuals victimized by male perpetrators)" [160].
	Charging fees could be exploitative	Victims could feel exploited if charged to use solutions	" ... the app was previously packaged with other apps that included We-Consent and charged fees [which] could seem exploitative" [157].
	Lack of utility	Solutions lack utility	" 'It just generally seemed like you could do the same things without the app, because iPhones nowadays are so intricate, you could click details on your messages and press 'send location' and type a short message. I feel like that wouldn't take nearly as long as opening the app, clicking the button, sending the messages. ... I think personally for me, it would just be easier to call or text them. It wasn't any easier to do that [using the app]' " [176].
	Mental state	Victims may not be in the right state psychologically	"Considering user's psychological profile: user's mental state could affect the effectiveness of the solution. While under duress and constant fear, it is inevitable that survivors might panic and struggle to use features that would normally be straightforward to use, or to miss certain precautionary routines" [118].
	The dynamism of relationships	Technological design does not account for the changes in relationships	"Social networking sites do not account for the dynamism of relationships, and assume that a "friend" on these sites stays that way" [93].

	Victim blaming	The design of some solutions encourages victim blaming	"Bystanders are encouraged ... to step up and prevent violent circumstances, but like many anti-violence initiatives, women are targeted in prevention efforts. Problematically, such applications are aimed at women as needing to be responsible for violence, rather than, for example, education initiatives that would target perpetrators of violence. That is, women are problematically expected to change their behavior by tracking their whereabouts and 'checking in' with friends to prevent violence" [39].
	Security and privacy concerns	There are security and privacy concerns with using some solutions	"Security breaches are a third area of significant threat, especially in light of the acutely sensitive nature of intimate data" [204].
	Lack of safety evaluation	The solutions are not evaluated for victims' safety	"It is recommended that some form of evaluation be built into these apps (beyond simply the number of downloads). It is also recommended that app developers give more consideration to the claims they make in their marketing and to give greater consideration to the ways their apps could be used in harmful ways" [37].
	Stereotype mentality	Solutions are designed with certain stereotypes in mind	"If [I'm] really in a (sexual abuse) emergency ... I feel like personally that would only happen if I were that drunk, and if I were that drunk, I don't know if I'd be able to use [the app]" [176].
	Lack of human support for victims	Solutions do not provide human support	"A particular challenge for an online intervention—if it is designed to be used without human interaction ... the young women felt that a web or smartphone app could not completely replace the "human touch" of real life support" [178].
	Stakeholder involvement	Stakeholders should be involved in the development of solutions	"Moreover, technologists interested in creating interventions that aid survivors ... must recognize that the technology cannot be developed in isolation. Instead, technical advances will need to be accompanied by parallel advances in legal and social support systems. For example, developing new techniques to collect legally valid digital evidence will require the legal system to evolve so as to recognize the new techniques" [79].
	Lack of usable solutions	Solutions are not usable for victims	"... survivors' stories demonstrated that the usability of privacy and security features is important, emphasizing findings from prior work focused on the general population ... in a higher risk context. For example, during the physical control and escape phases survivors benefited from access to technology to maintain communication with their support network, but they also wanted to hide those communications from an abuser who had physical access to them and their devices. But survivors faced high levels of stress and risk, which may have made it harder than usual for them to pay attention to user interface details. We observed that participants made mistakes when deleting or clearing information. Designers should therefore consider both the general usability of privacy and security features, and their use during high-stress, high-risk situations" [32].
	Technology maintenance	Technology is not maintained or updated	"Apps that are developed at a low level of sophistication — or apps that are developed at a high level of sophistication but are not well maintained — experience a lack of regular updates and poor data storage. Most ... apps are not regularly updated. Apps included in this review often contain links to outside sources (such as hotlines or advocacy resources) and apps that are not updated have a higher susceptibility to broken links and outdated information" [160].
	Lack of personalization of solutions	The solutions are designed as one-size-fits-all	"Diverse user needs and experiences of abuse. People's experiences of abuse and their journeys through that experience are complex. It is important to recognise that abuse can take place in any relationship, regardless of gender or sexuality. It can also take many forms, including coercive control, and psychological, physical, sexual, financial, and emotional abuse" [68].

TABLE A.2: Definitions and examples of sub-themes in our codebook on the theme of how technology assists victims.

3. How technology assists victims Evidence	Evidence gathering	The use of technology to gather evidence about a sexual abuse incident	"Evidence gathering via SNSs (social networking sites) ... the police using such sites to gather evidence for an investigation (such as collecting information about a victim or offender from their SNSs)" [101].
Challenges with evidence	Various technological sources	The gathering of evidence through multiple technological sources	"... what you may find is that they do it on Facebook, but they'll also be doing it on email, and will also be doing it on SMS. And so do you pursue all those different forums? Do you pursue enquiries with the telecommunication providers to determine when and where the emails were sent?" [87].
	Large amount of evidence	Difficulties with collating large amounts of evidence	"The sheer abundance of data generated by communication technologies ... poses investigators for a 'needle-in-a-haystack problem.' As the pool of publicly available information is nothing short of overwhelming, police work in this area is progressively becoming a big data research problem" [61].
	Ambiguous evidence	The gathered evidence is ambiguous	"Evidence collected through 'ambiguous' technological forms ... can be excluded before national Courts" [78].
	Revictimization	Revictimization in collecting evidence	" 'My concern ... is the idea that women have private and unrestrained access to their mobile phones ... having an app on your phone is the same as having the local women's aid card in your phone - you're asking a woman to make a risk assessment about whether it is safe to do so' " [37].
	Victim's responsibility to gather evidence	The responsibility of evidence gathering falls on the victim	"Victims feel that the responsibility of gathering evidence of the abuse is theirs, in order to avoid situations in which it is the victim's version of events versus the perpetrator's" [58].
	Lack of clarity on if consent is needed	Unclear if consent is needed to gather evidence	"... forum members are placing themselves at risk in order to gather evidence without knowing whether the recordings are admissible as evidence ... 'I'm wondering if without his consent it would be inadmissible in court as evidence' " [58].
	Stakeholder knowledge gaps	Stakeholders are not familiar with technology use cases	"Even in cases where police were successful in arresting and charging the perpetrator, police ... understanding of the techno-social aspects of the case impacted their decision to investigate and their advice to clients" [90].
	Unclear if consent was given	Unclear if consent is needed to gather evidence	"Evidence collected ... without compliance with the conditions provided by law can be excluded before national Courts" [78].

TABLE A.3: Definitions and examples of sub-themes in our codebook on the theme of the use of technological evidence in investigating abuse.

4. How technology assists victims and its challenges Government and technological service providers	Surveillance systems	The use of surveillance systems by the government to track victims and perpetrators	"Growing use of new technologies, including drones in the fight against human trafficking, is the EUROSUR (European Border Surveillance system) Regulation" [78].
	Hiding shelters in Google Maps	Hiding victim shelters in Google Maps	"Recognizing the impact of technologies on violent practices, NNEDV (National Network to End Domestic Violence) (2010) has advocated for increased safety measures with large technology corporations. Partnering with NNEDV, Google has begun to create user privacy and notification options for location-based services and worked closely with Google when the company launched 'Street View' to ensure that no undisclosed shelter appeared in Google Maps or Google Street View" [39].
Challenges with government and technological service providers	Legislative laws	Different laws exist in various jurisdictions	"Some cases demonstrated the challenges law enforcement face when the perpetrator or the content is outside local jurisdictions. For example, in one case a client's ex-partner was in Malaysia and threatened to disseminate her intimate images on social media. Police responded that they were unable to proceed as he was outside of the country. Similarly, in another case where the perpetrator hacked a client's Dropbox and posted her images onto local forums, police knew he was a 'serial uploader' yet they were unable to proceed as the sites were hosted in the US and therefore outside of SPF (Special Police Force) jurisdiction. ... These cases illustrate the long-observed challenges that law enforcement face when investigating technologically facilitated crimes. Often the perpetrator is outside their jurisdiction" [90].
	Privacy concerns with surveillance	Surveillance could raise privacy concerns for victims	"While tracking technology can certainly offer new opportunities to intervene ... it must be pointed out that being a form of surveillance it can be highly invasive on a person's privacy" [78].

TABLE A.4: Definitions and examples of sub-themes in our codebook on the theme of how government and service providers restrict abuse.