The author(s) shown below used Federal funding provided by the U.S. Department of Justice to prepare the following resource:

![Justice Information Resource Network]

Technology-Facilitated Abuse in Intimate Partner Violence (IPV): An Exploration of Costs and Consequences

Final Report

Principle Investigators:
Shaun M. Gann, Ph.D.
Senior Research Associate
sgann@jirn.org
(202) 503-3528

Mark Cohen, Ph.D.
Professor Emeritus
mark.cohen@vanderbilt.edu
(615) 322-0533

July 12, 2024

Technology-Facilitated Abuse in Intimate Partner Violence (IPV): An Exploration of Costs and Consequences: Final Report

Abstract

Technology-facilitated abuse (TFA) involves tools such as texting, mobile applications, smart devices, telecommunications networks, and social networks to bully, harass, stalk, or intimidate another person. In most cases, the perpetrator is usually someone the victim knows, often in the context of intimate partner violence (IPV). Perpetrators exploit the reach, connectivity, and anonymity of information technology services to commit a wide range of cybercrimes targeting specific individuals that can violate the victim's privacy rights, sense of well-being, and have a lasting, damaging impact on their lives. In partnership with Dr. Mark Cohen, the National Network to End Domestic Violence (NNEDV), the Cyber Civil Rights Initiative (CCRI), and IPSOS, the Justice Information Resource Network conducted a study to assess the costs and consequences associated with three types of technology-facilitated abuse within the context of IPV: cyberstalking, image-based sexual abuse (IBSA), and doxing.

The purpose of this project was to produce greater understanding of the harms victims and the public more generally suffer related to TFA within IPV, both those with tangible financial costs and harms that are intangible, with attention also paid to the experiences of minors. The goals were (1) to document the costs and consequences of three types of TFA (cyberstalking, IBSA, and doxing); (2) to estimate prevalence of these crimes via a nationally-representative, general population survey; (3) to provide willingness-to-pay estimates of their costs via discrete choice experiment (DCE); and (4) to use the results of achieving goals 2 and 3 to estimate the costs of cyberstalking, IBSA, and doxing to the United States.

This project was conducted in two phases. Phase I consisted of qualitative work to document the consequences to victims of the three forms of TFA in their complexity and interrelatedness. Activities included interviews with service provider professionals, subject matter experts, and survivor-advocates, a literature review, and three advisory board meetings. Phase II involved a nationally-representative, general population survey to estimate (a) the prevalence of TFA in the U.S., (b) the proportion of TFA that is associated with IPV, (c) cost values by asking respondents that disclose victimization about their out-of-pocket costs, and (d) DCEs to estimate the costs to society (i.e., the public's willingness-to-pay) associated with cyberstalking, IBSA, and doxing.

Table of Contents

List of Tables

Introduction

While technology can serve as a tool to protect survivors of domestic violence, stalking, and sexual violence, abusers often misuse it to harass, threaten, coerce, monitor, exploit, and violate their victims (National Resource Center on Domestic Violence, 2021). Scholars and victimization experts coined the term technology-facilitated abuse (TFA) as an umbrella phrase for these types of behavior. These crimes have potentially long-lasting and "comprehensive consequences" for individuals and their families, loved ones, and communities (Afrouz, 2021).

Although experts agree that TFA produces ongoing, detrimental effects for victims/survivors, there is a lack of definitional consistency regarding which behaviors fall under the TFA umbrella. This presents challenges in consistently identifying specific behaviors as abuses, identifying victims/survivors, enforcing the law in this area, measuring the prevalence of different types of TFA, and comparing estimates (Stevens et al., 2021).

Research in this area is still relatively new in the last 15 to 20 years—with the bulk of research less than 10 years old—and survey research has informed much of what currently is known. The reliability and validity of prevalence data on TFA is largely dependent on how researchers define behaviors and activities in these surveys, which may vary from study to study. For example, Taylor and Xia's (2018) systematic review identified 25 different conceptualizations of "cyber partner abuse" across the articles they reviewed (p. 988). Cyber partner abuse was their term for TFA perpetrated in the context of intimate-partner violence (IPV), which is IPV-related behavior using technology as the tool of perpetration; this is the scope of the present study as well. Dragiewicz et al. (2018) similarly coined the term "technology-facilitated coercive control" for the same phenomenon. The differences in terminology and levels of inclusiveness of various TFA-related behaviors demonstrate the need for definitional clarity for comparability between studies, something that is consistently challenging for research on nascent, evolving crimes.

Establishing definitions for these crimes was one goal of the current research, and the collaboratively developed, literature-based definitions chosen shaped the rest of the research. This definitional discussion follows below. The rest of this project focused on delineating the variety of harms and costs generated by three types of technology-facilitated abuse within IPV contexts: cyberstalking, doxing (public sharing of sensitive personal identifying information without the person's consent), and image-based sexual abuse (IBSA). As discussed below, we have limited the scope of IBSA for this project to three abuse types: (1) nonconsensual distribution of intimate images (NDII), formerly called nonconsensual pornography or "revenge porn" [1]; (2) sextortion; and (3) the sharing of sexually explicit digital forgeries, also known as "deepfakes." The final definitions informed the development of a taxonomy of harms and costs that result from these crimes and the design and conduct of a national survey that was used to

---

[1] This grant originally used the language "non-consensual porn" to describe what is commonly known as "revenge porn" and is now known as nonconsensual distribution of intimate images (NDII), which is a subset of image based sexual abuse (IBSA).

estimate the costs of these harms, prevalence rates for the three forms of TFA, and the frequency in occurrence of various harms enumerated in the taxonomy.

The purpose of this project, which is a collaboration between the Justice Information Resource Network (JIRN), the National Network to End Domestic Violence (NNEDV), and the Cyber Civil Rights Initiative (CCRI), is to produce greater understanding of the range of harms that victims, and the public more generally, suffer related to TFA within IPV—both harms with tangible financial costs and harms with more difficult-to-measure intangible costs. The objectives are: (1) to provide information about these harms that scholars and practitioners can use to support future research and practices to address these harms; and (2) to provide information about the scope of the problem and its costs to society. The goals are to: (1) document the consequences of cyberstalking, IBSA, and doxing; (2) estimate the prevalence of these crimes via a nationally-representative, general population survey; (3) provide per-respondent estimates of their costs via tangible cost reporting and willingness-to-pay (WTP) estimation methods; and (4) use the results of achieving goals 2 and 3 to estimate national costs of cyberstalking, IBSA, and doxing within IPV. By understanding more about the scope and distribution of these problems and their associated costs, more effective programmatic and funding decisions can be made to address these understudied forms of victimization and minimize their recurrence.

Research Questions

This research is therefore designed to answer several important research questions:

1. What are the prevalence and incidence rates associated with cyberstalking, IBSA, and doxing in the U.S.?
    a. What are the demographic profiles of these victims?
    b. Do these types of victimization occur more often in some parts of the country than others?

2. Within the context of IPV, what are the consequences and financial costs to victims associated with cyberstalking, IBSA, and doxing?
    a. What are the natures of these consequences, and how severe are they?
    b. How do these experiences differ for victims who are minors?

3. What is the estimated value of the costs typically associated with the consequences of cyberstalking, IBSA, and doxing in the U.S.?
    a. How much are people willing to pay (WTP) to avoid being victimized or to support remedies for these crimes?
    b. Is there significant variability in reported WTP based on prior victimization experience?

Links between TFA and IPV

While TFA can occur between strangers on the internet or between people in a variety of relationship types, TFA is an especially insidious tool when present in an intimate partner relationship. Dragiewicz, et al. (2018) described how abusers use technologies to increase the level of monitoring of their victims, instill fear and dependence of the victim on the abuser, and retaliate against their victims for perceived misbehavior. Cyberabuse is known to escalate to, or co-occur with, additional abusive behaviors including psychological and physical abuse and femicide (Brem et al., 2019; Brown et al., 2018), and "the same risk factors lie behind both online and off-line harms" (Finkelhor et al., 2020, pg. 1223). Furthermore, abusers engaging in TFA are likely to expand their abuse by committing cyberstalking, cyber sexual abuse, or cyber fraud against victims' loved ones, their workplaces, and other organizations that are important to them (Clevenger & Navarro, 2021). Dragiewicz (2021) has continued to emphasize the need to keep IPV at the forefront in discussions of TFA to accurately capture the frequency and repeated nature of victim and survivor experiences.

Technologies and online platforms have changed the nature of intimate relationships (Yardley, 2021). In addition to providing more ways to meet and communicate with intimate partners, "online disinhibition" can heighten and accelerate feelings of closeness; for example, partners may discuss sex more quickly than if they met in person (Almond et al., 2020). Teens especially may also expect their partners to immediately respond to messages and provide access to accounts as signs of trust (Baker & Carreño, 2016). While disinhibition can increase feelings of closeness and intimacy more quickly, it is also associated with technology facilitated IPV perpetration (Duerksen & Woodin, 2019) and can normalize surveillance as a part of intimate relationships (Levy & Schneier, 2020). Pitched as a way to enhance interpersonal connections, abusers can use these tools to extend their control of, and psychological violence against, their partners and ex-partners (Bianchi, et al., 2021; Lee & Anderson, 2016; Levy & Schneier, 2020).

However, like other forms of psychological and emotional abuse, when victims report TFA they often find that their experiences and concerns are dismissed or minimized (e.g., "It's not real" or "It's just Facebook drama") and it is not considered as serious or urgent as in-person physical or sexual abuse (Dunn, 2020; Gosse, 2021; Powell & Henry, 2019; Yardley, 2020). Nevertheless, it frequently co-occurs with and can lead to in-person violence outside the internet (Almond et al., 2020; Brown et al., 2021), and it can cause public humiliation, pervasive fear (Lee & Anderson, 2016), financial and reputational harm, and many other consequences.

Why TFA Constitutes a Unique Set of Crimes

Cybervictimization can cause unique harms that differ from those caused by other forms of offline victimization (Bailey & Mathen 2017; Citron & Franks, 2014; Dardis et al., 2019; Lee & Anderson 2016). Unique features of TFA are its pervasive, all-consuming nature because it can happen whether the abuser is physically present or not, leading to paranoia and the feeling that the perpetrator is always watching (Clevenger & Navarro 2021; Dardis et al., 2019; Henry et al., 2022; Lee & Anderson, 2016). For example, IBSA survivors have described the non-

consensual distribution of sexually explicit images as "torture for the soul" (McGlynn et al., 2021). Cyberstalking can affect all aspects of a survivor's life including school, work, social life, finances, and physical and mental health (Fissel, 2021). Doxing can harm survivors' reputations, remove the safety found in obscurity and anonymity, and increase abuse as more people are invited to participate in harassing the victim (Anderson & Wood, 2021). The normalization of "omnipresence" in relationships because of technology access (Yardley, 2021) leads to feeling that one cannot escape and that the abuse has no boundaries, which can amplify victims' levels of fear and hyperawareness/hypervigilance (Fiolet et al., 2021). Some IPV survivors even considered online abuse more harmful to their well-being than in-person assault:

> *"When I thought about rape victims before becoming one, I never thought that they were victimized after the rape. Not that the rape wasn't bad . . . Oh God no, it was. But I was constantly being victimized online and it was too much, you know. Like it never stopped and I couldn't do anything."*
>
> *Clevenger & Navarro, 2021, p. 365*

Features of technology platforms that invite others to witness, amplify, and replicate abusive posts or allow abusers to target more victims include the ease of sharing and replicating posts and the increased likelihood of further engagement with popular content (posts with a large number of clicks, views, and comments get "boosted" and seen by more people) (Gini et al., 2018; Lee & Anderson, 2016). Abusers often use online platforms to add to victims' fear and shame by abusing them in front of an audience (Woodlock, 2017) and inviting others to engage in the abuse (Douglas et al., 2019; Dragiewicz et al., 2019; Fiolet et al., 2021; Freed et al., 2017). Cyberstalking can be facilitated by tools that can be programmed to send harassing content regularly or remotely track a person's location and actions they take on their devices (Eterovic-Soric, 2017; Fraser et al., 2010). Recurring events compound psychological harm and emotional suffering (Bailey & Mathen, 2017; Dardis et al., 2019).

Existing laws are not yet sufficient to address TFA because not every state has specific statutes encompassing IPV-related crimes committed through technological means. The legal system may be hesitant to rule on cases involving TFA-related behaviors not explicitly defined under current laws, and First Amendment concerns about free speech online can come into play despite the impact of these behaviors on victims (Citron & Franks, 2014; Foley, 2021; Franks, 2017 & 2019; Levy & Schneier, 2020; Waldman, 2019). There is still a general lack of understanding in the legal system about what TFA is, why it matters, and how it manifests. The nature of these online activities is also difficult for courts to parse given that the current legal system jurisdictions are structured around geographically bound areas, while internet crime does not restrict itself to local jurisdictional boundaries. For example, websites may be hosted anywhere, and the medium does not require the abuser to be physically near the victim to perpetrate the abuse, making things like traditional restraining orders much more difficult to draft and enforce. TFA is unique because of its physical "spacelessness" and the ease, speed, and anonymity that technology affords the perpetrator(s) (Harris & Woodlock, 2019, p. 534).

How prevalent is TFA in IPV?

As cyber technology use has become ubiquitous, TFA is occurring more frequently (See e.g., Anti-Defamation League, 2022; Brady, 2017; Lee & Anderson, 2016; McGlynn, Rackley, & Houghton, 2017). Prevalence estimates vary widely. For example, rates varied from <1% to 78% across studies in one systematic review (Fernet et al., 2019), and a meta-analysis with a combined *n* of over 24,000 puts the estimate between 7 and 17% (Patel & Roesch, 2020).

Increased instances of TFA in recent years were reported to victim service providers around the world, and people of color, LGBTQ+ people,[2] and people with disabilities report experiencing higher rates of attacks as well as attacks that "specifically target their identities" (Dunn, 2020). Systematic reviews on interpersonal violence and abuse in adolescent intimate relationships have shown that 50–70% of youth reported experiencing IPV through technologies, depending on the acts included in each definition (Stonard et al., 2014). "Young people can experience up to 23 different incidents of cyber dating abuse in less than 6 months, with a predicted increase in the occurrence of such abuse given its indirect nature, the lack of geographic-temporal boundaries, and the frequent reciprocity of these acts" (Flach & Deslandes, 2017, p. 5). Abusive partners further increased online harassment and surveillance of their victims, and further restricted victims' technology access, during the COVID-19 pandemic in 2020 (Safety Net Project, 2021).

Although survivors and service providers have reported increased experiences of TFA in recent years and shared the devastation of experiencing it, few studies have produced reliable prevalence numbers based on common definitions and a comprehensive accounting of the various harms suffered by victims in the United States (Afrouz, 2021; Mumford et al., 2023; Rothman et al., 2023). Previous prevalence estimation attempts are explored more deeply below, along with their strengths and weaknesses.

Importance of Addressing the Harms of TFA

Addressing TFA cases is difficult and requires technical expertise (Afrouz, 2021; Matthews et al., 2017; Woodlock et al. 2020), knowledgeable and trauma-informed victim services, and law enforcement/court knowledge about technology and willingness to take on the cases. It is also difficult to have all copies of a post removed, meaning that total removal of content from the internet is never certain. Additionally, survivors may not always be aware abuse is happening, which means that friends, family, and employers may be seeing content they do not even know has been posted about them (Fiolet et al., 2021). Furthermore, TFA victims may experience harassment, threats, coercion, monitoring, exploitation, and other violations. Seeking help for TFA can consume survivors' financial, time, and emotional resources and rupture their employment, reputation, and social support systems.

---

[2] According to the Human Rights Campaign, LGBTQ+ is an acronym for "lesbian, gay, bisexual, transgender and queer" with a "+" sign to recognize the limitless sexual orientations and gender identities used by members of this community.

Needs have been identified across the victim response infrastructure for a better understanding of the serious harms caused by TFA and of the resources and best practices that can help victims and survivors. In Freed et al.'s (2017) study of family justice centers, professionals said that they did not have enough knowledge of technology to help survivors and that they "Google as they go" (see also Afrouz, 2021; Matthews et al., 2017; Woodlock, 2017). Others found that while many service providers encounter survivors of TFA, they do not always feel confident providing support and information on what survivors can do in the face of this kind of abuse (Fiolet et al., 2021; Gendera et al., 2021) or on how to increase their technology safety (Freed et al., 2017; 2018). Survivors themselves reported great support in rape crisis centers except when it came to cybervictimization (Clevenger & Navarro, 2021).

It is important to catalog and understand the full range of harms suffered by victims and survivors of TFA so that service providers and the criminal justice system can better serve victims and prevent future perpetration, and so that policy makers and legislators can allocate sufficient funds to support these efforts. Otherwise, survivor recovery will be hindered and more victims will lose their ability to participate in a society that increasingly operates online because they censor themselves or drop off altogether (Bailey & Mathen 2017; Citron, 2021). Powell and Henry (2019) further argue that greater attention must be paid to building the capacity of law enforcement to recognize the serious, long-lasting harms of TFA and to adequately respond to these crimes (see also Clevenger & Navarro, 2021; Vakhitova et al., 2021; SafetyNet, 2021).

> *"The surveillance of intimate life matters—not just because firms fail to provide notice or engage in deceptive practices but also because they undermine autonomy, dignity, intimacy, and equality… people's crucial life opportunities, including employment, education, housing, insurance, professional certification, and self-expression, are on the line. It matters because our core capabilities hang in the balance."*
>
> *Citron, 2021, p. 1771*

Furthermore, if TFA goes unchecked, some perpetrators may expand their activities from the private to the public sphere. Being rejected online leads some males to increase their aggressiveness toward the opposite gender (Andrighetto et al., 2019) and can lead some offenders to escalate into offline violence. Online misbehavior like doxing intimate partners can also increase the risk of radicalization (Braddock et al., 2021). Therefore, the impact of these crimes can extend far beyond their original context and their original victims, making the need to understand these crimes, how they manifest, the harms they cause, and the costs associated with these harms doubly important.

Why Study Costs of TFA

Understanding the economic impact of crime to victims, systems, and society has been a continuing concern to service providers, policymakers, and the public. Estimates of the fiscal burden of crime and the component harms that make up that cost are important, since the allocations of limited resources to address various crimes and between addressing crime vs. other social concerns are driven by these estimates (Maurer, 2017). The costs of IPV remain difficult

to estimate in general, and the introduction of technology to facilitate these abuses further complicates the process, since an abuser can perpetrate these activities outside of mere physical proximity to the victim. The unique consequences of cybervictimization in the IPV context have yet to be fully mapped out (Clevenger & Gilliam, 2020; Vakhitova et al., 2020).

To support future research and practice to address harms and reduce the prevalence of any given crime, information about the scope of the problem and its costs to society is critical (Cohen, 2020). Previous TFA research also reveals the need for a systematic understanding of victims' help-seeking behaviors, particularly considering the emergence of these new methods for perpetrating abuse, in order to identify service gaps (Bundock, et al., 2020; Dragiewicz, 2021). Afrouz (2021) argues that the lack of information and knowledge about the scope and impacts of IPV-related TFA hampers the ability address the true needs caused by these crimes.

Understanding more about the scope and costs of these problems will make it possible to make more targeted, informed programmatic and funding decisions to address these understudied forms of victimization. Additionally, these findings will guide efforts by invested parties, including victim services and criminal justice practitioners, victims, educators, employers, policy makers, technology companies, and others to address the needs of victims and reduce TFA perpetration. A more comprehensive understanding of the types of TFA and their costs and harms will also help in identifying best practices for victim assistance and in navigating the new technological and legal landscapes for IPV that have been complicated by the introduction of specific technology-facilitated forms of abuse. Contributing to this body of knowledge for practice as well as to the growing literature on this emerging realm of abuse is a primary goal of this research.

Present Report

To begin to address the problem of TFA in intimate partner relationships, and to design effective policies and interventions to do so, we must understand the size of the problem and its impacts. This report combines (1) a review of previous research and data collections, (2) interview data from practitioners, researchers, and survivors of TFA, and (3) findings from a nationally-representative survey to examine the nature of these abuses; evaluate prior estimates of the prevalence of IBSA, cyberstalking, and doxing; the tangible and intangible consequences of TFA for individuals, their networks, their communities, and society; and previous uses of cost analysis research in TFA and crime generally. Relatedly, we also identify measurement issues that could affect the construction of victimization prevalence and cost estimates such as definitions used and time horizons included.

This report therefore proceeds as follows. First, previous work on TFA including definitions of cyberstalking, IBSA, and doxing is presented along with the final definitions for each crime chosen for this project. These are followed by victim and perpetrator-associated theories of TFA. Next, previous attempts to measure the prevalence of these crimes are discussed along with their strengths and limitations, followed by a discussion of cost estimation methods that build upon the previous work completed by JIRN and partners for their previous NIJ-funded study, "Estimating the Financial Costs of Crime Victimization" (Lugo et al., 2018). Next, we

present two products: the taxonomy of costs and harms of TFA and the final national survey instrument. Finally, we present results from analysis of the survey data, with a particular focus on the prevalence and incidence of three forms of TFA, as well as the costs and harms associated with TFA victimization.

Methods

Literature Review. Initial searches were conducted during May 2021 in EBSCO databases (Criminal Justice Abstracts with Full Text; Psychology & Behavioral Sciences Collection; SocIndex with Full Text; and Index to Legal Periodicals & Books Full Text) and Google Scholar. Additional literature searches were conducted periodically until March 2024. Search results were limited to items from 2016-present in the English language. Literature was focused on prevalence estimates and consequences of victimization for cyberstalking, IBSA, and doxing, all within the context of romantic relationships.

Existing datasets related to these topics were also assessed for their utility in understanding the prevalence and costs of these crimes, such as the National Crime Victimization Survey (NCVS), the NNEDV survey on cyberstalking, CCRI surveys on NCP (e.g., Eaton, et al., 2017), the National Intimate Partner and Sexual Violence Survey (NISVS), the Youth Risk Behavior Surveillance System (YRBSS), the Internet Crime Complaint Center (IC3), and other potentially relevant datasets related to intimate partner violence (IPV) across disciplines.

All ages were included (adolescents, emerging adults, and adults). Search strategies included intimate partner violence-related and technology-related terms (e.g., digital, online, cyber) within the subject field; intimate partner violence-related words near technology-related terms; and additional searches of the three specific forms of TFA with intimate partner words (e.g., dating, relationship, boyfriend, girlfriend) and victimization-related words. Additional reports and articles were recommended by subject matter experts on our advisory board and were also found during reviews of victim organization websites (Center for Victim Research, National Network to End Domestic Violence/SafetyNet, VAWnet of the National Resource Center on Domestic Violence, and the National Sexual Violence Resource Center). Database searches related to cost estimation methods for crime were conducted in August 2021. Search terms included "cost of victimization," "cost benefit analysis," "willingness to pay," and "discrete choice model/experiment." Finally, table of contents alerts and newsletters (like CrimPapers) and Google scholar alerts provided ongoing updates to results.

As of March 2024, these search criteria returned 319 articles, reports, and book chapters for review. Results were excluded if they were not original studies, original data collections, metanalyses, or systematic reviews on TFA prevalence or the nature, consequences, or impacts of TFA victimization, or they were not methodological works on estimating costs of crime. Research was also excluded if cyberstalking, doxing, or IBSA was primarily committed by someone other than an intimate partner (e.g., fellow students, online trolls, or workplace colleagues). Additional targeted searches were then undertaken to fill identified gaps or to ensure that new publications were included. 225 sources on TFA, its prevalence and harms, and on cost

estimation were ultimately included in the final literature review. Most eligible research originated in the United States or Australia.

Interviews and Advisory Board Discussions. In addition to reviewing previous literature, the project team interviewed 17 subject matter experts (SMEs) on TFA to gather the best current thinking in the field, especially from practitioners and survivors. Eight of these interviewees also served on the project advisory board and helped to recruit the rest of the interviewees via snowball sampling. SME interviews took place virtually between August and October 2021. All interviewees provided their informed consent to participate before their interview and all but one person gave their consent for the interview to be recorded.

Of the 17 interviewees, 47% ($n = 8$) self-identified as subject-matter experts in cyberstalking, 18% ($n = 3$) were experts in image-based sexual abuse, one was an expert in multiple areas (cyberstalking and IBSA), one was an expert on doxing, and one person's expertise was in intimate partner violence more broadly. Three interviewees self-identified as TFA survivors. Interviewees were asked questions about their areas of expertise, the accuracy of various contentious definitions of IBSA, cyberstalking, and doxing, and the various harms suffered by victims of these crimes. The interview instrument is provided in Appendix 2. These interviews were coded for thematic analysis and analyzed in Nvivo; the results of these interviews are woven throughout the relevant discussions below.

The Advisory Board met three times during this stage of the project. Group discussions were facilitated related to definitions of these three forms of TFA and the project scope (how broadly to conceptualize these crimes and how that could impact the project), harms and costs of these forms of TFA, and discussion of an early draft of the general population survey presented at the end of this report. The first two meetings occurred on November 5th and 8th, 2021, and the third meeting occurred on February 1, 2022. Input provided during these collaborative meetings was also categorized by themes and is woven throughout the relevant discussions below.

Survey Methodology. The detailed survey methodology—including sampling and weighting—is discussed below and in Appendix 3.

Background on Technology-Facilitated Abuse

Definitions

Research examining TFA has conceptualized these abuses and behaviors in a variety of ways. This has important implications for the identification of these crimes as well as criminal justice and victim service policy and practice. As survey research provides the basis for much of what is known about these types of abuses, our understanding of TFA is largely attached to how researchers describe behaviors/activities in surveys. For example, on the most basic level, cyberstalking involves the use of technology to repeatedly communicate with, harass, or threaten a victim(s) (Wilson et al., 2022). IBSA is a broad term that includes several different crime and abuse types that relate to the "nonconsensual creation and/or distribution of private, sexual images," including forms of voyeurism, surveillance, and upskirting (McGlynn & Rackley, 2016). As discussed in more detail below, we have limited the scope of IBSA for this project to three abuse types: (1) nonconsensual distribution of intimate images (NDII), formerly called nonconsensual pornography or "revenge porn" [3]; (2) sextortion, or the "threat to distribute one's real or synthetic intimate material without that person's consent if the person does not comply with certain demands" (https://cybercivilrights.org/faqs/#terminolog); and (3) the sharing of sexually explicit digital forgeries, also known as "deepfakes." Finally, doxing has been defined as the public release of a victim's private, sensitive, personal information (Franks, 2016). These and other definitions for the three evolving TFA behaviors examined in this study are described in more detail below with a particular focus on the lack of consistency across studies.

A review of previous literature provides insight into the complexities of comparing findings related to these abuse types across studies given these definitional inconsistencies. Some studies limit the number of abusive behaviors included in their definitions. Furthermore, overlapping abuse behaviors can place them within multiple categories or under different umbrellas (e.g., sextortion and doxing, as discussed below), and definitions are constantly evolving as the understanding of these types of abuse becomes more informed. One example is a Bureau of Justice Statistics report intended to capture technology-facilitated stalking behavior. However, the report also included items from the 2019 Supplemental Victimization Survey (SVS) to the NCVS that described behaviors related to doxing and/or image-based sexual abuse (see Morgan & Truman, 2022). For example, respondents were asked, "Has anyone ever posted or threatened to post inappropriate, unwanted, or personal information about you on the Internet, including private photographs, videos, or spreading rumors?" (Morgan & Truman, 2022, p. 14). This is but one example of the difficulties in isolating types of TFA victimization from each other.

Dragiewicz and colleagues (2019) further refine the definition of technology-facilitated abuse by distinguishing between what they call "technology-facilitated coercive control" and

---

[3] This grant originally used the language "non-consensual porn" to describe what is commonly known as "revenge porn" and is now known as nonconsensual distribution of intimate images (NDII), which is a subset of image based sexual abuse (IBSA).

other forms of technology-based abuse, crime, and bullying. The authors identify a common thread among "technology-facilitated coercive control" behaviors in that they involve "violence and abuse by current or former intimate partners, facilitated by information and communication technologies or digital media, acknowledging technological aspects of abuse in the context of coercive and controlling intimate relationships" (Dragiewicz et al., 2019, p. 8; see also, Dragiewicz et al., 2018; Harris, 2018). Although the authors identified several behaviors that fit within their definition of technology-facilitated coercive control, they noted that there are often overlapping behaviors across each of them.

In the present study, we hope to contribute to the body of literature on the definitions for these crimes, as settling on final definitions for behaviors included and excluded will shape the entire study. Our first step in defining technology-facilitated cyberstalking, doxing, and IBSA was to present the definitions of each of these abuses provided in the original NIJ solicitation from the extant literature to the panel of SME interviewees and ask them whether the definitions accurately captured these abuses, such as specificity in their descriptions of behaviors and whether perpetrator intent should be included. These findings will be discussed in more detail below in the treatment of each form of TFA, but overall, the consensus was that all three definitions lacked clarity, particularly regarding the acts that constitute the type of abuse, and that more specificity is needed in the language. The lack of consistency in definitions ultimately has implications for understanding the prevalence of these behaviors and the harms caused to victims, according to the 17 SMEs.

The following sections present discussions of previous definitions and the debates about what should be included in definitions for each form of TFA. The final definitions chosen for use in the survey conclude this section.

Cyberstalking

With the prolific growth in the technology industry over the past several decades, a variety of new media and communication platforms have increased the methods and ease of interacting with individuals across the world. While the use of these platforms has been linked to many positive experiences, scholars have acknowledged a negative side associated with the excessive use of internet and social media platforms (Kaur et al., 2021). Technology provides access to individuals looking to infiltrate deeper into others' lives that can facilitate stalking behaviors (Reyns & Fissel, 2020). One of the major challenges in research on cyberstalking is the lack of consensus among experts in the conceptualization and operationalization of cyberstalking as a distinct phenomenon (see Kim, 2023; Kaur et al., 2021; Dhillon & Smith, 2019; Fissel, 2019). Specifically, there is some debate as to whether cyberstalking should be considered a subset or extension of traditional stalking. Scholars have identified similarities in the consequences and harms of both types of stalking (Reyns & Fissel, 2020).

Cyberstalking has previously been defined as the repeated use of electronic communications to stalk a person (Witwer et al., 2020, p. 3). As frequency of cyberstalking has increased with advances in technology, scholars and practitioners within the victimization and victim services fields have begun to refine this definition to provide more behavior-specific

language, and some include descriptions of the perpetrator's intent and the harms caused by these behaviors (SME Interviews; see also Reyns & Fissel, 2020; Wilson et al., 2022). Cyberstalking perpetrators have an array of technologies they can use for unwanted contact with a victim(s) on- and offline. For example, they may send or post offensive messages online or follow, monitor, or track a victim's location and activities (Flynn et al., 2021; Fraser et al., 2010). While the term cyberstalking is more synonymous with internet communications technologies, other technologies such as global positioning system (GPS) trackers, keystroke loggers, hidden cameras, webcams, and audio bugs can also be used (Eterovic-Soric, 2017; Fraser et al., 2010). Furthermore, offline stalking is often interrelated with online stalking victimization (Reyns & Fisher, 2018), and studies have found that online stalking is most prevalent in the contexts of family and domestic violence (see Brem et al., 2019).

Cyberstalking has therefore been defined in different ways depending on the behaviors included, which creates problems for researchers and policy makers when speaking to the prevalence of this abuse as well as for identifying best practices to prevent or minimize risks to potential victims. Eighty percent of the SMEs interviewed for this study (12 of 15) indicated that the use of the term stalking is unclear and may lead to confusion in interpreting its intended meaning. The SMEs indicated that stalking implies overtness, but covert monitoring and surveillance is more common. The SMEs also suggested that the use of the word communications in definitions of cyberstalking is missing the fact that these acts are not limited to communications (e.g., location tracking).

Therefore, it was recommended that definitions should replace "communications" with "electronic means." Other definitions have specified that not only must the behavior be repetitive, but it must also be viewed by the victim as unwanted communication or contact. Some experts have also added language to depict the emotions that this behavior evokes for a victim to the descriptions of included behaviors. Specifically, cyberstalking is expected to bring about negative emotions among victims such as helplessness, concern, distress, and/or fear (Al-Rahmi et al., 2019; Nobles et al., 2014; Maple et al., 2012).

In discussing differences between covert actions and overt actions considered to be cyberstalking, the SMEs provided a set of examples to highlight the major differences. Covert actions may involve monitoring (e.g., devices, messages, locations); changing authorization functions on devices or enabling unauthorized functions; impersonating the victim to run up debts, interfere with relationships, and/or cancel important events; social engineering (e.g., manipulating victim's family into providing information to use against the victim); or isolating victim(s) from social connections. Overt actions may involve: sending abusive messages to victim(s); incessantly contacting victim(s) about their child(ren); speaking poorly of victim(s) online; calling law enforcement and presenting as the victim to incite an arrest; calling/harassing the victim's bosses and colleagues about the victim; sending messages to victim's new partner (sometimes posing as the victim); or provoking victims until they respond emotionally and then filming them and using it against them (e.g., in court) (SME Interviews).

Scholars and experts have also distinguished between cyberstalking and other types of TFA (e.g., cyber harassment). Specifically, the National Conference of State Legislators (2016) suggests that cyberstalking differs from cyber harassment in that the former poses a credible

threat of harm to the victim. Similar findings emerged from the interviews with subject matter experts: interviewees indicated that the word cyberstalking is often used in a casual manner, so it is important to contextualize the risks, threats, and escalation of danger in the criminal definition. Three SMEs also indicated it is important to specify that malicious intent is a key aspect of cyberstalking and that definitions of cyberstalking should aim to specify that the intent driving this behavior is to shame, humiliate, harass, or incite others to do the same; others stated that inserting intent into a criminal definition can create problems for proof.

These definitional disagreements highlight the challenges to identifying the extent to which this type of TFA occurs, the potential solutions to preventing it, and the ability to identify victims/survivors. Furthermore, these definitional differences create an issue of generalizability across studies when researchers use variations of the aforementioned definitions. SMEs stated that the quantity of contacts should not determine what behaviors are considered cyberstalking, but rather, the focus should be on the intensity of contact(s) and threats of harm/violence. The SMEs proposed revising the definition of cyberstalking to the following: "Cyberstalking is the repeated use of electronic means via the internet or technology to stalk, monitor, or surveil a person with the intent to shame, humiliate, harass, or incite others to do the same." Although not part of the recommended definition, some SMEs also indicated that a more gendered approach may be needed to highlight the fact that victims/survivors are predominately female. It may also be important to consider manipulation of others as a proxy to monitor the target (e.g., children of separated parents).

Image-Based Sexual Abuse (IBSA)

Image-based sexual abuse (IBSA) is another type of TFA that is targeted either directly or indirectly at a person or group of persons. IBSA, or NDII/NCP, has been defined as when nude or sexually explicit images are distributed without one's consent. Similarly, Eaton and colleagues (2017) defined IBSA/NCP as the distribution of nude or sexually explicit images or videos of a person without their consent. The authors note that these images and/or videos may have been consensually produced and/or obtained in the context of an intimate partner relationship. It is also possible that these materials were produced and/or obtained without the consent of the individual(s) involved. Either way, these materials are distributed by an individual without the consent of the victim.

As apparent in the description of NCP by Eaton and colleagues (2017), NCP involves more than produced media pornography, and these nuances have implications for who is identified as a victim/survivor. The SMEs interviewed as part of this study indicated that the term IBSA covers both NCP (*actual* distribution) and sextortion (*threats* to distribute images or videos), both of which can have devastating effects on the victim (see also McGlynn & Rackley, 2017). Further clouding the definitional waters, it is important to note that IBSA is considered by some to be a form of doxing, while others have defined it as a separate crime.

IBSA takes a variety of forms and includes behaviors such as voyeurism and "upskirting," sextortion, NDII, and the creation of "deep fake" sexual images and videos (Eaton & McGlynn, 2020; SME Interviews). Deep fakes involve constructed or digitally manipulated

images (Eaton & McGlynn, 2020) and were identified by the SMEs as increasing in prevalence. The SMEs also noted that deep fake images/videos can be just as harmful as real images/videos. The SMEs suggested that using the term IBSA opens the door to capture other similar types of behaviors that may have not been captured previously. The term IBSA also shifts the focus from distribution to the experiences of victims.

As mentioned above, the older term nonconsensual pornography is sometimes still described as synonymous with the term "revenge porn" and used in media reports and scholarly publications (Goldstein, 2020; Gavin & Scott, 2019; Lageson et al., 2019). However, scholars have suggested that using these terms interchangeably has important implications for who is identified as a victim (Witwer et al., 2020). More specifically, "revenge porn" implies that a perpetrator is motivated by a personal desire to get revenge on a victim. Therefore, this excludes victims on the basis that the behavior was motivated by financial gain, bragging, entertainment, and so forth. The term nonconsensual pornography is more general in the sense that it does not delineate a particular motivation that drives the behavior. Witwer et al. (2020) described that nonconsensual pornography was adopted by the field as a broader substitute for the term revenge porn for this reason. The SMEs further noted that it is important to include a statement on the coercive control that serves as a major driver of this TFA behavior, which is why threats to distribute images or videos are often used to coerce the victim into desired behaviors, such as sending more images, performing sexual favors, or staying in an unwanted relationship. These sextortion threats are included under the IBSA umbrella along with NCP, as they are deeply interrelated.

The SMEs provided further description of the behaviors, actions, and offender characteristics that should be used to classify incidents as IBSA. The SMEs indicated that IBSA perpetrators can be divided into one of two groups: a main NDII offender who initiates the distribution of material, and others (typically strangers) who redistribute the material. Acts by the main offender may include publicly disseminating intimate images or videos to revenge porn websites, the victim's personal and social networks, and the victim's employers, for example. Furthermore, the offender may use or create intimate images or videos to threaten and/or acquire something such as money or sexual acts, to impersonate or pose as the victim, and possibly to invite violence towards them. Acts by others or strangers may include saving the images or videos, distributing them to people who do or do not know the victim, and/or violating the victim's privacy (e.g., sending explicit photos of themselves to the victim, sexually propositioning the victim, or showing up at the victim's house).

A recently published manuscript takes a closer look at the prevalence of online sexual offenses against children in the United States (Finkelhor et al., 2022). A nationally representative sample of young adults were asked about their experiences of online and TFA during their childhood. Although the survey included a variety of items related to online and TFA, the authors were also interested in identifying prevalence rates for several cross-cutting concepts (e.g., online child sexual abuse; image-based sexual abuse). The authors captured IBSA using responses from multiple survey items that included misuse of images, threats or pressure to obtain images, voluntarily provided images in a statutorily impermissible relationship, and the provision of images for commercial purposes. Responses to the items on the forced image category and the voluntarily providing images to an older partner were only counted if images

were actually provided to the perpetrator(s).

As previously mentioned, the SMEs recommended moving away from the term NCP or revenge porn to the more inclusive term of IBSA (see also, McGlynn & Rackley, 2017). The interviewees noted that the term pornography sexualizes the abuse when the motives may vary (e.g., revenge, coercive control, extortion, having "fun," or to gain status within social groups). These definitional considerations reveal the challenges to capturing consistent information related to NCP as well as the more inclusive term of IBSA.

Doxing

Doxing occurs when an individual's personal contact or other sensitive or identifying information is published on the internet or distributed to others via electronic means without consent. Doxing is another form of technology-facilitated abuse that has garnered increasing national attention, especially during recent United States elections. Illustratively, an internet search using the terms "doxing" and "U.S. election" will return several hundred thousand results. Doxing can also occur within the context of an intimate partner relationship.

Similar to other TFA behaviors, there are slight variations between definitions in use. For example, one scholar defined doxing as the nonconsensual release of private and/or sensitive "personal identifying information" about an individual into the public domain (MacAllister, 2017, p. 2451). Note the subtle differences between the opening definition and this one: "personal contact or other sensitive information" vs. "personal identifying information," which could include a multitude of ways to identify someone. One definition might lead a researcher to include the sharing of sensitive images or private information about the victim's life whereas the other might not. These variations have important implications for who is identified as a victim as well as prevalence estimates.

Doxing may also involve different actions and levels of engagement, including: an act of releasing information; an act of doing something with that information; and an act of spreading the information with the intent of creating a cyber mob. Acts of releasing personal information may involve distributing personally identifying information such as social security number, addresses, phone numbers, workplaces, and names of family members. Acts of doing something with the acquired information may consist of generating mass phone calls; harassing the victim's employer(s); sending the victim things (e.g., pizza deliveries); opening credit cards in the victim's name; and speaking ill of another person, threating them, or embarrassing them online.

Anderson & Wood (2021) noted that while most doxing research focuses on political, activist, hacker, and crypto-market circles, intimate violence perpetrators have also used doxing to delegitimize their victims through the targeted release of personal information that was shared confidentially with them (such as sexual orientation or HIV status). For example, abusers may release private or sensitive information about a victim to their family, friends, and employer(s). To this point, doxing is neither effective nor useful to a perpetrator unless there is an audience (SME Interviews). Alternatively, perpetrators of doxing may distribute personal information about a victim to facilitate abuse by others. For example, they might create fake internet profiles

that present the victim as a sex worker, leading them to be harassed by individuals seeking sexual services (Freed et al., 2018; see also MacAllister, 2017). While the SMEs noted that there are similarities and a statistical association between IBSA and doxing, they suggested that these are distinct crimes/abuses which should be reflected in the definitions.

The SMEs also indicated that there are certain aspects of doxing behaviors that are important to include in its definition. Specifically, they suggested that in some instances it might be difficult to identify what constitutes doxing or what could also apply to regular websites that gather/distribute personal information for marketing purposes or that might be characteristic of a data breach. Like the other TFA behaviors, the SMEs noted the importance of including intent to harm a specific individual in the definition. Ultimately, the SMEs recommended revising the definition of doxing to read as follows: doxing is when an individual's personally identifying information (e.g., home/work address, phone number, social media, financial information, etc.) is published on the internet or otherwise distributed to others via electronic means without their consent with the intent to cause harm. As with the other definitions, the final definition used in the survey is presented below.

In addition to the inclusion of these specific elements, the SMEs identified several important features of doxing that may be worth considering. The interviewees indicated that doxing refers to what people do with the information; however, once the information is out in the public domain, it also becomes part of the threat to victims—that there is the possibility that someone may use it and that possibility has a mental and emotional impact on the victims. There are also some common differences in perpetration of doxing based on the perpetrator's age. Specifically, the SMEs indicated that sharing personally identifying information is more common among adults, whereas with adolescents, sharing private or sensitive information that could cause shame is more common. Lastly, the SMEs indicated that doxing is one tool used by perpetrators among an arsenal of other types of TFA harassment that may be co-occurring.

Previous Pitfalls in Definitions

Prior research examining TFA has identified a variety of issues associated with the definitions of these types of behaviors. Stevens and colleagues (2021) conducted a systematic review of the cyberstalking and cyber harassment literature and suggest that discrepancies across definitions likely contributes to varying prevalence estimates of these behaviors as well as problems with victim/survivor identification. Similar findings and observations emerged from the interviews with the SMEs regarding definitional issues.

Taylor and Xia (2018) conducted a systematic review of the literature on what they called cyber partner abuse (CPA). The authors found that "conceptualizations of CPA varied with minimal uniformity...a total of 25 terminologies for CPA were used in the reviewed articles" (p. 988). They identified that about 50% of included studies were more inclusive of different electronic platforms and abusive behaviors in their definitions, but studies even varied in how they categorized these behaviors (e.g., direct threats, control or monitoring, insults, direct aggression). Differences in the behavior-specific language of definitions have direct implications for victim identification, which may cause over- or under-reporting in prevalence estimates.

There was a strong consensus among the SMEs that TFA is not limited to instances where the victim and perpetrator have had physical contact or prior/current intimacy. Specifically, the SMEs suggested that these behaviors can be perpetrated by someone either currently or formerly known to the victim closely, casually, or even hardly at all, and the connection may or may not have involved physical contact or intimacy. The extant literature and the SMEs indicated that the concept of "intimate partner" should be broadened to encompass any meaningful relationship as defined by the victim. Such broadening may serve to capture occurrences perpetrated by neighbors, roommates, a person with whom the victim has gone on a single date or multiple dates, cohabitating partners (whether married or not), and those who have separated after a dating or partner relationship. Further, it may include intimate relationships that arise virtually even when there is no contact in person.

Context, intent, and impact matter when defining and examining TFA. Experts have suggested that behaviors such as monitoring or accessing accounts could be considered normal and necessary for some relationships (Carlson & Frazer, 2021; Levy & Schneier, 2020). Individuals may not see these behaviors as a violation of their privacy. Scholars further identify that there may be a generational divide in how individuals interact with technology as well as perceive certain technology-related behaviors. For example, adolescents may expect monitoring as a normal part of relationships or think of these behaviors as "annoying," but not abusive (Baker et al., 2016). Similarly, some victims may not be as bothered by or fearful of the same behaviors as other victims may be (Vakhitova et al., 2021). Lacking context about the behavior or how it is understood can contribute to overcounting behaviors that may not be considered harmful or abusive by specific individuals or individuals from different cultures (Dragiewicz, 2021, SME Interviews).

The lack of uniformity in definitions across studies examining TFA is not limited to specific behaviors. Clevenger and colleagues (2018) noted that there are inconsistencies in definitions across a variety of abuse types, such as cyber intimate partner abuse, cyberstalking, cyberbullying and cyberaggression, and cybersexual exploitation that can include IBSA, but also commercial sexual exploitation of children or child pornography.

Lastly, it is important to recognize some of the differences and similarities in these three technology-facilitated abuses, which should be considered when selecting definitions for each. The SMEs provided some final thoughts related to these. One notable difference in these three behaviors is that cyberstalking is usually perpetrated by an individual who knows the victim, whether casually or deeply, whereas doxing and IBSA are more likely to involve additional people who do not know the victim due to widespread distribution and resharing of material. This distinction should be reflected in the definitions. In terms of similarities, the SMEs indicated that all three forms of TFA can be executed through direct actions of the perpetrator or through involvement of a third party (e.g., using children to monitor the partner's activity or location, or by inciting others into a "cyber mob"). All three TFA behaviors are also used as forms of control, intimidation, harassment, and/or humiliation of the target. Research has also indicated that each of these behaviors may be used for the purposes of exploitation (see also Clevenger et al., 2018).

Final Definitions

The research team selected definitions for each of the three cybercrimes covered in this review. These definitions were informed by the prior research, and behaviorally specific examples were also developed to provide additional context. These definitions were piloted in the cognitive tests of the final survey instrument for conceptual clarity and understanding by individuals at a variety of reading levels. The final definitions presented here are used in the nationally representative survey component of this project.

Cyberstalking. We define cyberstalking as when someone uses technology to repeatedly harass another person, surveil them, or monitor their activity and causes them to feel afraid. This may or may not be accompanied by offline or in-person activity. The following examples highlight various forms of cyberstalking:

1. Unwanted and repeated texting, emailing, or social media messaging.
2. Monitoring of social media, email, financial, or other accounts and communications. Can include using their logins to access their accounts, monitoring their published posts to track their activities, or the use of stalkerware/spyware that the individual installs on the person's phone or computer.
3. Changing log-in information or security settings on a person's devices.
4. Impersonating a person to run up debts, interfere with relationships, and/or cancel important events (like court dates).
5. Monitoring a person's location via technology.

Image Based Sexual Abuse (IBSA). Image-based sexual abuse (IBSA) includes several different kinds of harmful acts. These include dissemination, or threatening to disseminate, a partially nude, nude, or sexually explicit image or video without the consent of the person depicted. Sometimes those images are real, while other times a perpetrator has manipulated or fabricated the images using software, AI, or other technology to make it appear as if the person depicted is nude or engaged in a sex act. Listed below are several behavior-specific scenarios:

1. Someone threatened to post partially nude, nude, or sexually explicit images of a person online unless they agreed to do something against their will (e.g., pay $500, send more nude images, stay in a romantic relationship against my wishes, etc.). The perpetrator eventually stopped bothering them and none of the images were distributed.
2. Someone threatened another person as described above. The perpetrator ultimately *did* distribute the images without their consent through chatting apps and text messages to friends, posted them online, and/or sent hard copy images through the mail to the individual's family.
3. Someone posted partially nude, nude, or sexually explicit images of another person on websites without their consent. The perpetrator never threatened the individual before posting and they only learned of what happened afterward.

Doxing. Doxing is defined as someone releasing another person's personal contact or other sensitive, identifying information to others or the public via electronic means, without the individual's consent. Other individuals may also have acted on this information after it was

published, such as by creating a cyber mob to harass or attack the individual, making mass phone calls, opening credit cards in their name, or showing up at their house.[4] Examples of doxing include:

1. Publishing someone's phone number or social media accounts online and inciting others to harass or threaten that person.
2. Distributing someone's work or school address, home address, social security number, social media handles, medical information, sexual history, or financial information to others via electronic means without their consent.

Theory

Research on intimate partner TFA is still in its infancy. While there has been a surge of research on TFA generally, fewer studies have specifically focused on TFA in the context of intimate partner relationships (however defined). Researchers in this area have applied common criminological and victimization frameworks to intimate partner TFA, with the overwhelming majority employing offender-focused theories to explain it (e.g., lifestyle-routine activities theory). These theories attempt to explain victimization by identifying factors that increase the likelihood that an individual will engage in antisocial behavior resulting in victimization and providing insight into perpetrator decision-making processes.

Victims' unique social positions might influence how and why they may be selected as targets for TFA (Afrouz, 2021). On the other hand, victim-focused theories center on the experiences of victims and how they contribute to the potential for future re-victimization and/or negative victim outcomes (e.g., polyvictimization theory). These theories also have important implications for the study of associated costs. This section will provide a brief overview of each set of these theories as they apply to TFA within the context of intimate partner relationships.

Victim-Focused Theories

Polyvictimization Theory. Scholars have taken a particular interest in how past experiences in victims' lives give way to future experiences/behavior. Drawing from other fields, especially psychology, researchers have begun to consider the relevance of polyvictimization theory as a possible explanation for negative mental health and behavioral outcomes among victims who experienced cyber victimization.

Cyber victimization is generally associated with several types of maladaptive behaviors, including depression-related symptoms and antisocial behavior (e.g., theft, weapon-carrying, drug use; see Tennant et al., 2015; Wright & Li, 2013; Mehari et al., 2020). While this is important to framing how polyvictimization may impact intimate partner TFA, polyvictimization

---

[4] *Note:* this does not include mass data breaches, which would be when hackers steal your private information from a credit card company.

theory shifts the focus away from differences in victim outcomes to identifying whether and why victims may have had exposure to multiple episodes or different types of victimization over time (Davis et al., 2018; Ford et al., 2010).

More recently, scholars have identified several limitations of polyvictimization theory and have made recommendations to advance its potential explanatory power (Davis et al., 2019). Davis and colleagues note that "consistent with polyvictimization theory's emphasis on the need to expand the search for risk factors beyond the type of victimization alone, it is important to avoid focusing solely on the presence or absence of polyvictimization as a risk factor" (p. 166). Rather, the authors suggest that researchers should consider the characteristics of specific victimization experiences that may be associated with increased risk for negative outcomes. Scholars have identified several characteristics that may serve to amplify the harm caused by victimization, which include a trusted perpetrator, perceived life threats, and negative social reactions (see Delker & Freyd, 2014; Ozer et al., 2003; Trickey et al., 2012; Ullman, 2010). Therefore, polyvictimization theory is best applied to understanding the risk of re-victimization and adverse behavioral outcomes.

Conservation of Resources Theory (COR). Conservation of resources theory posits that trauma and victimization can lead to losses of valuable resources for the victim; losses that must be mitigated to prevent further loss and to promote healing and recovery (Bath, 2008; Hobfoll et al., 2016; Littleton et al., 2009; Sullivan, 2016). COR has been adapted by scholars and applied to explain the trauma of intimate partner violence victimization (Sullivan, 2016; 2018) and has been used as a social and emotional well-being promotion framework to better design responses to victims' needs. Sullivan (2016) explains that survivors of IPV experience specific resource losses upon victimization that further contributes to additional resource loss and impacting the victim's wellbeing. Resources lost may include tangible items (e.g., money or possessions), intangible sources of strength (e.g., self-esteem, confidence in one's ability care for oneself or one's family), or specific conditions (e.g., a safe home) (see Halbesleben et al., 2014; Littleton et al., 2009).

Scholars have applied COR to examine a variety of victimization outcomes (e.g., cybervictimization in the workplace and intimate partner violence; see Alahmad & Bata, 2021; Anwar et al., 2020; Sauber & O'Brien, 2020). Sauber and O'Brien (2020) analyzed data from 147 female domestic violence survivors who recently experienced abuse by a male partner. The authors found that psychological, physical, and economic abuse were related to posttraumatic stress, depression, and loss of economic self-sufficiency. Losses of financial, work, and interpersonal resources were significantly related to the aforementioned outcomes and were stronger predictors of victim wellbeing changes than variables capturing the abuse experiences (such as economic sabotage or economically controlling behaviors), suggesting that resource loss and the ability to weather it may be a mediating factor between suffering abuse and the severity of some victim outcomes. Although no study to date has applied COR to the study of TFA, COR may be particularly useful in advancing the knowledge regarding the mechanisms through which TFA relates to psychological and financial stress suffered by victims/survivors and their recovery trajectories. Findings from this research could have policy and practice implications for responding to the unique needs of victims of TFA.

Feminist/Gender Theories. Feminist scholars have long emphasized the importance of the power and social status that is afforded to males which can create inequitable situations and social status for females (Dobash & Dobash, 1979). This is particularly noted for females in heterosexual relationships; in some instances, men may exploit this power to perpetuate violence against female partners. Scholars have maintained that the socialization of norms surrounding heterosexual relationships and traditional forms of authority are correlated with IPV (Johnson, 2008; Brown et al., 2018). More recently, scholars have noted the need to create a more fluid conceptualization of gender so that it does not exclude violence among individuals in LGBTQ+ communities or minimize violence directed toward males (Hunnicutt, 2009).

Research has demonstrated that females are disparately represented in prevalence estimates of IPV and TFA and that they experience disproportionate levels of harm from these abuses (see Marwick & Miller, 2014; Reed et al., 2016; Anti-Defamation League, 2022). Research of online harassment has revealed that perpetrators commonly target women and other marginalized groups (Marwick & Miller, 2014). Reed and colleagues (2016) found that high school girls who experienced online abuse from a dating partner were significantly more likely to report higher levels of emotional distress and negative emotional responses when compared to male victims. Researchers also found an association between female victims who experience offline IPV and the likelihood of experiencing online abuses—particularly among victims at higher risk for injury and homicide (Reed et al., 2016; Marganski & Melander, 2015). This research provides a framework for understanding why some victim subgroups might be at higher risk for TFA victimization than others.

Perpetrator-Focused Criminological Theories Applied to TFA

Lifestyle Routine Activities Theory. Lifestyle Routine Activities Theory (L-RAT) is the most commonly applied theory used to study intimate partner TFA perpetration (Fissel, Fisher, & Wilcox, 2023). This theory emphasizes the importance of an individual's daily activities and how those impact one's likelihood of becoming victimized. An inherent assumption underlying L-RAT is that motivated offenders select targets by weighing the perceived risks and benefits of engaging in a crime (Cohen & Felson, 1979). L-RAT considers how certain activities in victims' daily routines increase the risk of victimization due to closeness to motivated offenders and a lack of guardianship. L-RAT is comprised of both lifestyle exposure theory and routine activities theory.

Routine Activities Theory (RAT) was proposed by Cohen and Felson (1979) and attempted to explain how changes in everyday activity patterns influence crime rate trends in the post-World War II era. The perspective suggests that crime is most likely to occur when motivated offenders, suitable targets, and a lack of capable guardianship converge in time and 'space.' Researchers have more clearly stated that the convergence of these elements largely depends on the structure of normal, daily activities (see Messner & Blau, 1987). Cohen and Felson (1979) found that the increase in crime rates during the 1960s and 1970s was largely attributable to changes in social life. For example, criminal opportunities increased in the post-WWII area partly because women began to heavily join the workforce. This change, among others, resulted in more time spent away from the home and increased criminal opportunities for

those who might target them.

Lifestyle exposure theory indicates that the probability of victimization is likely to increase as a function of how much one's lifestyle (or behaviors) increase the amount of time spent in spaces among strangers (Madero-Hernandez, 2019). These lifestyle activities are associated with increased risk of victimization because individuals are exposed to potential offenders in situations without effective crime prevention restraints. Based on an analysis of data from eight American cities, Hindelang et al. (1978) concluded that the probability of victimization is related to an individual's lifestyle. Engaging in activities such as work and school, or leisure activities such as socializing and 'play,' are key predictors of victimization.

Both theories are known as incentive theories (or theories of opportunity) because victimization is considered a by-product of illegal opportunities that are present in everyday life (Abu-Ulbeh et al., 2021). Miethe and Meier (1994) describe the primary differences between these theories as being the language that is used and the focus used to describe victimization risk. Although there is some debate about the compatibility or similarities between these theories (see, Choi, 2008; Reyns, 2015), many have concluded that combining these theories has face validity, since taken together they have consistently been shown to predict the probability of victimization (e.g., Cohen et al., 1981; Vakhitova et al., 2016; Abu-Ulbeh et al., 2021). L-RAT contends that victimization events are mostly likely to occur when individuals are in high-risk situations, close to motivated offenders, viewed as a suitable target, with a lack of capable guardianship protecting them (Cohen & Felson, 1979; Miethe & Meier, 1994). However, Vakhitova and colleagues (2016) noted that these main concepts are not evident in the original models and that how these are defined may depend on the researchers.

Criminological research to date has primarily examined the explanatory power of L-RAT in the context of victimization in the physical world. More recently, studies have begun examining the relevance of L-RAT in explaining cybervictimization. Yar (2005) critiqued the applicability of L-RAT to cybercrime because virtual environments are spatially and temporally disconnected. Nevertheless, researchers have explored whether L-RAT accounts for variation in the probability of victimization in the virtual world; one could argue that the risk factors of motivated offenders, exposure as a suitable target, with a lack of capable guardianship exist in online as well as offline spaces—perhaps even more so, even if the characteristics of risk vary.

The outcomes of interest in this study involve three virtual crime types that have received relatively little scholarly attention (IBSA; cyberstalking; and doxing). Of these, cyberstalking has received the most attention among scholarly studies examining L-RAT and cybercrime victimization. Some scholars are simply including doxing among other behaviors to define "cyber abuse" (e.g., name-calling, trolling, doxing, open and escalating threats, vicious sexist, racist, and homophobic rants, attempts to shame others, and direct efforts to embarrass or humiliate people; see Duggan, 2014; Vakhitova et al., 2016) rather than as its own crime. These definitional issues and other previously mentioned critiques of L-RAT in explaining TFA should be considered when interpreting the findings from studies using the L-RAT framework.

Social Learning Theory. Social learning theory (SLT) posits that individuals engage in crime because they learned the behavior (Akers et al., 2016). There are four ways that antisocial

behaviors are learned according to SLT. First, individuals can learn behaviors through *differential association*, in which individuals learn the values, attitudes, techniques, and motives needed to engage in antisocial behavior by interacting with others. Second, individuals are more likely to engage in antisocial behaviors if they are exposed by family and friends (*imitation*). Third, *differential reinforcement* affects the likelihood that individuals will continue engaging in or desist from engaging in antisocial behavior. This occurs when individuals are either rewarded or punished for engaging in a behavior. Lastly, people are more likely to engage in antisocial behavior if they learn *favorable definitions* toward it; in other words, people orient their behaviors around whether they view the behavior as being (un)desirable.

Research has provided some support for SLT to explain some forms of cybercrime (e.g., cyberstalking). Van Ouytsel and colleagues (2017) examine the relationship between SLT and the perpetration of digital monitoring behaviors among a sample of adolescents. Specifically, the authors had measures of imitation (e.g., controlling behaviors perpetrated by father and/or mother) and differential association (e.g., acceptance of dating abuse among friends). The findings indicated that acceptance of dating abuse among friends and controlling behaviors perpetrated by the respondents' fathers were significantly related to cyberstalking perpetration. On the other hand, controlling behaviors by the respondents' mothers was not associated with cyberstalking behaviors.

General Strain Theory (GST). General strain theory is distinguished from other strain theories in that strain can come from sources other than poverty and socioeconomic status (Agnew, 1992). GST posits that strain can result from any relationship or event when an individual perceives that they were not treated as expected or have an undesirable experience or outcome. This may include a relationship or event in which an individual fails to achieve positively valued goals, there is the threat of or removal of positively valued stimuli, or there is the threat of or experience of negatively valued stimuli (Agnew, 1992, p. 50). These sources of strain can increase the likelihood that an individual experiences negative emotions associated with crime (e.g., fear, anxiety, depression, anger; Agnew, 1992). It is important to note that GST recognizes that strain does not always result in an individual engaging in crime; sometimes it can lead an individual into prosocial corrective actions.

The application of GST to TFA is best suited for offenses that involve anger, jealousy, hatred, or a desire to seek retaliation or revenge (Hay & Ray, 2020). Hay and Ray (2020) summarize the theoretical arguments for applying GST to study a variety of cybercrimes, including cyber dating abuse. The authors adopted their definition of cyber partner abuse from Zweig and colleagues (2014) which is "the control, harassment, stalking, and abuse of one's dating partner via technology and social media" (p. 1306). Furthermore, the authors highlight that GST is relevant to the aspects of these crimes that involve a desire for revenge or retaliation driven by anger, insecurity, jealousy, and rejection (see also Curry & Zavala, 2020).

Self-Control Theory. Self-control theory assumes that individuals are rational decision-makers in the economic sense, in that individuals use their available knowledge when deciding to engage in behaviors (i.e., bounded rationality; Gottfredson & Hirschi, 1990). Bounded rationality recognizes constraints around the level and nature of information available to a given individual for decision making at any point in time, which has implications for the behaviors that a person

chooses. More specifically, individuals weigh the potential benefits of a certain behavior against potential risks associated with it. The level of known information has the potential to distort decision-making, in that an individual may choose to engage in an act that they perceive as being pleasurable or beneficial rather than painful or risky, even if the true risks and benefits would imply a different conclusion.

Gottfredson and Hirschi (1990) make the case that individuals with deficits in self-control (i.e., low self-control) are more likely to view crime as attractive. Low self-control is associated with risk-taking, impulsivity, lack of empathy, and preferences toward simple and/or physical-oriented tasks. Self-control, they argue, is the singular trait related to an individual's propensity toward criminal behavior. Additionally, self-control is developed early in life and remains stable after the age of eight. Self-control is developed and dependent on successful parental management, which includes emotional attachment to the child, effective parental monitoring, evaluating the child's behavior, and applying effective behavioral management techniques.

Although the focus of self-control theory is on criminal offending, Gottfredson and Hirschi (1990) acknowledge the fact that there is a relationship between self-control and victimization. Specifically, they indicate that the risk of victimization is related to the characteristics of self-control associated with criminal offending. It is the inability of individuals to effectively weigh the risks and benefits of behavior that increases criminality as well as risk of victimization. Stated more simply, individuals with low self-control are more likely to expose themselves to risky situations, associate with deviant peers, and behave in a dangerous manner which increases their risk of victimization.

So far, self-control theory has been applied in studies examining cyberstalking. Similar to stalking in the offline world, cyberstalking is a short-sighted behavior that satisfies a perpetrator's immediate desire to know about someone else's whereabouts, personal associations, and lifestyle activities (Giggins & Nicholson, 2020). Individuals with low self-control are unable to recognize the consequences of their behavior, both to themselves and to others. For example, perpetrators of cyberstalking are not considering the trauma that is experienced by the victim, but rather the immediate benefits gained from engaging in this behavior and knowing where they are. Research has found an association between low self-control and cyberstalking behaviors (see, for example, Reyns et al., 2012).

Theoretical Summary

Traditional criminological and victimization theories have begun to be applied to the study of TFA. Victim-centered theories focus on explaining the experiences of victims, how victims perceive these experiences, and how they may contribute to future (re-)victimizations. These theories are therefore central to understanding the costs and harms of experiencing TFA. On the other hand, criminological theories focus on explaining the motivations for perpetrating TFA. Much of the research in this area has applied offender-focused theories to explain TFA (e.g., lifestyle-routine activities theory). L-RAT attempts to explain victimization by considering the factors that increase the likelihood an individual engages in antisocial behaviors or risky situations, which increase the risk of victimization. Additionally, criminological theories such as

social learning, general strain, self-control, and bounded rational choice provide insight into the decision-making process of perpetrators of TFA behaviors as well as some unique victimization vulnerabilities. Victims' unique social positions in relation to others and in their online behaviors might influence how and why they are selected as targets by perpetrators of TFA, especially when an intimate partner relationship is involved (Afrouz, 2021). Potential relationships between some of these theories and TFA victimization will be explored in some of the hypotheses tested using the survey data from this project.

Previous Attempts to Measure Prevalence

Research on the prevalence of TFA is still in its infancy (Clevenger & Gilliam, 2020). As such, estimates of TFA and its various forms tend to vary widely. For example, in one systematic review of cyber intimate partner victimization in adolescent girls and women, TFA prevalence rates ranged from less than 1% to as high as 78% across the studies included (Fernet et al., 2019). Throughout the literature, a major factor affecting TFA prevalence estimates is how TFA and its subcomponents are defined. More concise definitions will typically lead to lower prevalence estimates, while vague or wide-ranging definitions, especially when used in conjunction with self-report surveys, will lead to larger estimates. Further difficulties in estimating the extent of TFA arise when considering methodological issues regarding reporting, monitoring, and even recognizing these actions as crimes (see below).

According to two recent systematic reviews, estimates of TFA prevalence vary significantly (Fernet, 2019) and can conflict when disaggregated for gender differences in rates of victimization and perpetration (Taylor & Xia, 2018), to name one complexity. This section discusses and provides summary tables for previous attempts to measure the prevalence of TFA in the extant literature. We first discuss TFA in general, as many studies do not differentiate its various forms in their estimates. We then present and discuss the prevalence estimates for each of the three types of TFA included in this project: IBSA, cyberstalking, and doxing.

General TFA Prevalence

A large portion of published studies combine multiple technology-related abuses into a single prevalence measure of TFA as opposed to separating it into its various forms. For example, in the Pew Research Center's nationally representative survey of online harassment, their measure of TFA includes physical threats, sustained harassment, stalking, and online sexual harassment. Naturally, studies that include a measure of "any TFA" tend to produce, on average, higher prevalence estimates relative to those that examine a single type. Table 1 shows a variety of these more blanket TFA estimates.

General TFA prevalence rates vary significantly depending on the behaviors included in the TFA measure and the composition of the study sample. Among the 13 studies included in the table below, TFA prevalence rates ranged from 10% (direct cyber aggression among a sample of U.S. adults aged 19-30: Borrajo et al., 2015) to 84% (cyberabuse among 216 men arrested for domestic violence: Brem et al., 2019). These rates illustrate the importance of definitions and

sample construction when estimating TFA prevalence. Without consistent definitions of TFA and its various forms, it will be quite difficult—if not impossible—to develop accurate and valid estimates of a crime that appears to be increasing as the use of Internet-connected devices is more widespread (Clevenger et al., 2018).

In partnership with NNEDV, NORC conducted a nationally representative survey with 2,752 young adults between the ages of 18 and 35 in the United States to assess respondents' experiences with TFA during their lifetime (Mumford et al., 2023; NORC, 2022). Approximately 70% of respondents indicated that they have experienced TFA at some point in their lifetime. Their definition of TFA quite broad, including the three most prevalent responses: "Checked my phone call histories without my permission" (29.4%); "sent me unwanted pornographic or obscene images or messages via email, text, social media, or another online platform" (28.8%); and "checked my phone call history without my permission" (25.9%). By themselves, none of these behaviors would be considered IBSA or cyberstalking as defined in this study. The results also revealed that prevalence estimates are higher for individuals who identify as trans or non-binary compared to cis-gendered women or men. In fact, 86% of respondents who identified as trans or non-binary experienced TFA in their lifetime. Furthermore, a greater percentage of respondents who identified as LGBTQ+ indicated they had experienced TFA in their lifetime (81%) compared to individuals who identified as heterosexual (68%).

The Anti-Defamation League (ADL)'s annual survey on online hate and harassment takes a close look at whether victims from different marginalized populations are overrepresented in estimates of online harassment generally, but their definition may or may not involve an intimate partner (Anti-Defamation League, 2022). Specifically, the survey results reveal that individuals from marginalized groups were significantly more likely to report having experienced severe online harassment during their lifetime than non-marginalized populations; whereas a similar percentage of marginalized and non-marginalized respondents indicated that they had experienced some form of online harassment during their lifetime. Compared to other racial/ethnic subgroups, Hispanics were the most likely to report having ever experienced online harassment (40%) followed by Asian Americans (39%), Jewish Americans (37%), Blacks/African Americans (34%), and Muslim Americans (33%). This pattern shifts slightly when considering reports of having ever experienced severe online harassment with Asian Americans reporting the highest levels (31%) followed by Blacks/African Americans (27%), Muslim Americans (26%), Hispanics (24%), and Jewish Americans (23%). An overwhelming majority of respondents from each of these racial/ethnic subgroups reported that their experiences of online harassment were the result of hate-based harassment (i.e., physical appearance, gender, race or ethnicity, religion, sexual orientation, gender identity, or disability). Lastly, respondents from marginalized populations were more likely than respondents from non-marginalized populations to report that their victimization experiences were the result of their race/ethnicity (26% and 24%, respectively).

Table 1: General TFA Prevalence Estimates by Victim Group

Category	Type of TFA	Prevalence Rate	Sample	Source
Adults	Interpersonal violence, harassment and/or abuse that is conducted using a phone, online, and/or digital technologies	50%	N=4,562 Australian adults Nationally representative sample	Flynn, Powell, & Hindes, 2023
Adults	Misuse of technology to harm, harass, threaten, coerce, exploit, or violate a person (including invasion of privacy such as checking phone call history without permission	70%	N=2,752 U.S. adults aged 18-35	Mumford et al., 2023
Adults	Severe online and digital harassment (sexual harassment, stalking, physical threats, swatting, doxing, & sustained harassment), whether intimate partner involved or not	27% 12% 1-year rate	N= 2,300 adults Nationally representative sample	Anti-Defamation League, 2022
Adults	Severe online behaviors such as physical threats, sexual harassment, stalking, and sustained harassment	18% of Americans	N=4,248 Nationally representative sample	Duggan, 2017 (Pew Research Center)

Category	Type of TFA	Prevalence Rate	Sample	Source
Adults	Interpersonal violence, harassment and/or abuse that is conducted using a phone, online, and/or digital technologies	50%	N=4,562 Australian adults Nationally representative sample	Flynn, Powell, & Hindes, 2023
Adults	Cyber dating abuse: monitoring/ surveillance *or* aggressive behavior (rude or humiliating comments, sending emails or threatening messages, posting photos with the intention to humiliate)	10-14% suffered direct aggression 70-82% suffered cyber monitoring or surveillance	N=788 U.S. adults 19-30 who had been in a relationship at some point	Borrajo, Gámez-Guadix, Pereda, and Calvete, 2015
Adults	Cyber surveillance, cyber-interference, reputational harm, monitoring/tracking, fraud, controlling/limiting access	81%	N=504 sexual and gender minority (SGM) adults 18-35 in the U.S. (taken from a nationally representative sample of 2,752 U.S. adults)	Vogler, Kappel, and Mumford, 2023
Adults/ Adolescents	Intimate partner digital abuse (being purposefully embarrassed online, being called offensive names, and being stalked)	12%	N=2,810 Nationally representative sample of Americans aged 15 and above	Ybarra, Price-Feeney, Lenhart, and Zickuhr 2017
College Students	Intimate partner cyber aggression (i.e., using text messages or social media to harass a partner)	75%	N=540 college students who had been in a relationship in the past year	Marganski and Melander 2018

Category	Type of TFA	Prevalence Rate	Sample	Source
Adults	Interpersonal violence, harassment and/or abuse that is conducted using a phone, online, and/or digital technologies	50%	N=4,562 Australian adults Nationally representative sample	Flynn, Powell, & Hindes, 2023
College Students	Technology-facilitated partner abuse	~50% reported perpetrating or experiencing	N=433 N=804 N=219	Borrajo, Gámez-Guadix, and Calvete, 2015; Burke, Wallen, Vail-Smith, and Knox, 2011; Martinez-Pecino and Durán, 2019
Adolescents	Severe online/ digital harassment (sexual harassment, stalking, physical threats, swatting, doxing, sustained harassment), whether intimate partner involved or not	25%	N=500 Nationally representative sample of American adolescents aged 13-17	Anti-Defamation League, 2022 (same survey as above, different sample component)
Adolescents	Digital dating abuse (looked through contents of device without permission; kept you from using their device; threatened via text; posted something publicly online to make fun of, threaten, or embarrass you; posted or shared a private picture of you without permission)	28.1% of teens who had been in a romantic relationship in the past year	N=2,218 Nationally representative sample of middle and high school students aged 12-17	Hinduja & Patchin 2020

Category	Type of TFA	Prevalence Rate	Sample	Source
Adults	Interpersonal violence, harassment and/or abuse that is conducted using a phone, online, and/or digital technologies	50%	N=4,562 Australian adults Nationally representative sample	Flynn, Powell, & Hindes, 2023
Adolescents	Cyber-control (excessive control behaviors) and cyber-aggression (threats and insults through social media)	Cyber-control: occasional 30.5%; frequent 13.6% Cyber-aggression: occasional 4.1% frequent 7.5%	N=604 teens aged 12-17 in Spain who were in romantic relationships at the time or in past 12 months	Cava et al., 2020
Adolescents	Interpersonal violence and abuse through technologies	12 - 56% across 12 studies (dependent on definitions and behaviors included)	Evidence synthesis of 56 studies from 2000-2013 including 12 studies of Cyberabuse	Stonard et al., 2014
Men	Cyberabuse (i.e., sent threatening texts to partner, checked social network page to monitor partner)	81% perpetrated cyberabuse 84% reported being victimized by cyberabuse	N=216 men arrested for DV and court-referred to batterer intervention programs in RI	Brem et al., 2019

Cyberstalking

The majority of stalking estimates come from studies that focus on traditional or "offline" stalking; relatively few prevalence estimates are available for cyberstalking (Clevenger et al., 2018). Studies indicate, however, that there is a significant amount of overlap between the two types of victimization. For example, Baum and colleagues (2009) found that approximately 20% of traditional stalking victims were also victims of cyberstalking. Table 2 shows a comparison of the cyberstalking estimated discussed below.

According to the 2016 National Crime Victimization Survey's Supplemental Victimization Survey, 3.8 million persons 16 years old or older in the U.S.—or 1.5% of this

population—were victims of stalking (Truman & Morgan 2021). This decreased to 3.4 million (1.3%) in the 2019 survey (Morgan & Truman 2022). Behaviors included in "stalking with technology" included unwanted phone calls, voice messages, and text messages; unwanted emails/messages using the internet or social media; monitoring of activities using social media, posting/threatening to post inappropriate/unwanted/personal information,[5] spying on or monitoring activities using technology, and tracking whereabouts with an electronic device/application. Most of those persons reported experiencing both stalking with technology and traditional stalking (0.6%), though a greater percentage reported experiencing stalking with technology only (0.4%) than traditional stalking only (0.3%). Furthermore, of those who reported being stalked with technology only, 54.3% of perpetrators were known to the victim (17.6 were identified as intimate partners), 19.3% were strangers, and 26% were unknown. These estimates look quite different for individuals who reported both experiencing traditional stalking and stalking with technology. Eighty-one percent indicated that the perpetrator was known to them (with 35.5% indicating that it was an intimate partner). Approximately 12.2% reported that the perpetrator was a stranger and 6.6% indicated that they were unknown.

The National Intimate Partner and Sexual Violence Survey (NISVS) conducted by the Centers for Disease Control and Prevention (CDC) also captures data on TFA behaviors related to cyberstalking (Smith et al., 2022). The NISVS is an ongoing, nationally representative survey of adults in the United States. Although the survey does not capture prevalence rates of stalking victimization by type (i.e., physical vs. technology-facilitated), the survey does ask about the tactics experienced by stalking victims. This provides some insight into whether stalking victims experienced TFA or were physically stalked.

In general, Smith and colleagues (2022) report that 1 in 3 females and 1 in 6 males experienced some type of stalking victimization during their lifetime. Of the females that experienced stalking, 75.5% experienced unwanted calls, 55.9% received unwanted texts, photos, or emails through social media, 16.7% were tracked or monitored by GPS, and 8.8% were spied on through the use of technology. Similar patterns emerged for male victims in that 75.3% experienced unwanted phone calls, 60.7% received unwanted texts, photos, or emails through social media, 20.5% were monitored or tracked through the use of GPS, and 11.7% were spied on through the use of technology.

Additionally, the Online Hate and Harassment survey is a national-level survey conducted by the Anti-Defamation League, which captures data on a variety of TFA-related behaviors. This annual survey is a nationally representative, web-based survey designed to capture data on online hate and harassment-related behaviors (ADL, 2022). The 2022 results are based on responses from 2,330 Americans aged 18 and older. The sampling frame oversamples for individuals from Jewish, Muslim, Black or African American, Asian American, Hispanic, Latinx, and LGBTQ+ populations. Overall, they estimated a 12% lifetime prevalence and a 4% 1-year incidence rate.

---

[5] See discussion on page 13 under definitions about whether this behavior is really cyberstalking.

Table 2: Cyberstalking Prevalence Estimates by Victim Group

Category	Type of Cyberstalking	Prevalence Rate	Sample	Source
Adults	Repeated pursuit using communication technologies causing a substantial emotional response	31.8%	mTurk Survey N=1,500 adults aged 18-25	Fissel, 2019
Adults	Been stalked online	10% 4% 1-year rate	N=2,300 adults Nationally representative sample	Anti-Defamation League, 2022
Adults/ Adolescents	Stalking with technology (e.g., monitored activities using social media, tracked whereabouts electronically, phone calls, voice/text messages)	1% in 2019 80% of all stalking victims	Nationally representative NCVS samples of Americans aged 16 and above	Morgan & Truman, 2022
Adults/ Adolescents	Varied by study	3.7 to 82%, variances were definition-dependent	Systematic review of 43 studies	Stevens et al., 2021
College Students	Repeated online pursuit behaviors causing worry about personal safety	3.4%	N=1,987 college women	Reyns, Fisher, & Randa 2018
College Students	Repeated harassment, unwanted sexual advances, threats of violence	41%	N=541 college women	Reyns, Henson, and Fisher, 2012
College Students	Repeated harassment through electronic means	9%	N=471 undergraduate and graduate students	Kraft & Wang, 2010

The ADL survey asks respondents about a variety of behaviors, two of which may be considered cyberstalking, though not necessarily by an intimate partner. Respondents were asked whether they have been *harassed* online for a sustained period during their lifetime and in the past 12 months. Approximately 11% of respondents indicated that they have experienced online harassment during their lifetime, with 4% indicating that these experiences occurred within the past 12 months. A greater percentage of respondents who were identified as being from a marginalized population were harassed online (12%) compared to non-marginalized populations

(9%). Females were slightly more likely than males to report being harassed online during their lifetime (12% and 11%, respectively). Respondents were also asked whether they have been *stalked* online in the past 12 months or during their lifetime. Similar to sustained harassment, approximately 10% of respondents indicated they have been stalked online at some point during their lifetime and 4% reported being stalked online in the past 12 months. Respondents from marginalized populations were also more likely to report being stalked online during their lifetime (12%) compared respondents from non-marginalized populations (6%). Both males and females were equally likely to report being stalked online during their lifetime (10%)

Some studies have found that younger individuals may be more likely to report cyberstalking, but comparing these estimates is again hampered by inconsistent definitions. For example, Reyns et al., (2012) examined a sample of undergraduate students from a large Midwestern university and found that 41% had experienced cyberstalking at least once in their lifetime, with females (46%) significantly more likely to be victimized relative to males (32%). Similarly, Fissel (2019) surveyed 1,500 U.S. adults aged 18-25 and found that, within the past year, approximately 32% had been a victim of cyberstalking, which was defined as "the repeated pursuit by the same person (2 or more times) of an individual using communication technologies that would cause a reasonable person to experience a substantial emotional response or feel fear for their safety or the safety of someone close to them" (p.77).

The lack of a consistent cyberstalking definition has had a considerable impact on prevalence estimates (Fissel, Reyns, Nobles, Fisher, & Fox, 2024). Stevens et al. (2021) conducted a systematic review of the cyberstalking and cyber harassment literature and found that numerous definitions of cyberstalking were used among the included studies. A major delineation among the definitions was how many times an action must occur before it is deemed stalking. They argue that this definitional issue is the most likely contributor to the exceedingly large range of prevalence estimates found amongst the studies in their review, which ranged from 3.7% to 82%. A more recent scoping review that incorporated 41 quantitative and qualitative studies found a cyberstalking victimization prevalence range of 0.7% to 85.2% (Wilson, Sheridan, & Garratt-Reed, 2023).

IBSA

For this study, we limited the scope of IBSA to include the threat of (sextortion) or actual dissemination (NDII) of partially nude, nude, or sexually explicit images or videos without the consent of the person depicted, including those that are inauthentic ("deep fakes"). As shown in Table 3, the primary difference in IBSA definitions revolves around whether the image/video was shared privately (i.e., amongst the perpetrator's friends) or publicly (i.e., on a website). A large percentage of sexually explicit images/videos are shared with other private parties, though there are numerous websites dedicated to nonconsensual pornography or revenge porn—as many as 3,000 according to Clevenger et al. (2018)—to which IBSA perpetrators can upload images and/or videos.

Like the other types of TFA, the prevalence estimates of IBSA tend to be highly variable depending on (1) the definition used and (2) the characteristics of the sample (Walker & Sleath,

2017). For example, Marganski and Melander (2018) used a sample of college students and defined IBSA as privately or publicly sharing an explicit image or video. The authors found that 6.3% of the sample had been victimized in the past 12 months. Conversely, Dick et al. (2014) examined youths aged 14-19 and defined IBSA as only the public sharing of an explicit image (not video). They observed a 1.5% IBSA prevalence rate among those included in the sample. Scholars have also attempted to obtain estimates of childhood experiences of IBSA. Finkelhor and colleagues (2022) found that 11% of young adults (ages 18-28) reported having experienced an episode of IBSA during their childhood (ages < 18 years old); they included misuse of images; threats/pressure to obtain images; voluntarily provided images to older partner; and commercial talk, images, or other sexual activity in their definition of IBSA.

Walker and Sleath (2017) conducted a systematic review of 82 IBSA (revenge porn and nonconsensual pornography) studies published between 2010 to 2017. Among the adult samples included in their review, the IBSA prevalence rate ranged from 1.1% (ever experienced) to 6.3% (experienced in the past 12 months). In the three youth studies included, prevalence rates varied from 1.5% (whole sample, previous three months) to 32% (those who admitted to "sexting," ever). Interestingly, among the adult studies that presented findings based on gender, the IBSA victimization rates were higher for males (1.8% to 10.4%) than for females (0.5% to 3.3%), though the difference was statistically significant in only two of the included studies.

The Cyber Civil Rights Initiative (CCRI) published a report in 2017 that summarized the findings of their survey on nonconsensual pornography (NCP) victimization using a sample of U.S. adults recruited through Facebook (N=3,044; Eaton et al., 2017). CCRI (2017) captured NCP by asking "Has anyone ever shared or threatened to share a sexually-explicit image or video of you without your consent?" (p. 11). Results indicated that 12.8% of survey respondents had been a victim at some point in their life. More specifically, 8% of respondents had their sexually explicit material shared, while another 4.8% had been threatened but their material was never shared. Furthermore, the age distribution of NCP victimization resembled a modified age-crime curve, with victimization rates increasing in early adulthood, peaking between ages 26-33, and steadily decreasing as age increased (Eaton et al., 2017).

Eaton and colleagues (2017) also asked respondents about their NCP perpetration, if any. Overall, 5.2% of the sample reported that they had ever knowingly disseminated a sexually explicit image or video without consent. Consistent with prior research, males (7.4%) were over twice as likely than females (3.4%) to be NCP perpetrators (Eaton et al., 2017). Unlike NCP victimization, there was no pattern in perpetrators' age. Young adults aged 18-25 reported the highest levels of NCP perpetration (8.2%), followed by those 34-41 (5.6%), 50-57 (5.4%), and 42-49 (4.5%).

As previously mentioned, the Online Hate and Harassment survey conducted by the Anti-Defamation League is a nationally representative survey that asks respondents to report on TFA-related victimization experiences. Although not clearly defined in the data, the survey asks respondents to report on their experiences of online sexual harassment. While online sexual harassment may involve other non-IBSA behaviors (e.g., sexualized bullying, unwanted sexualization), it may include the non-consensual sharing of intimate images and videos. Approximately 10% of respondents reported being sexually harassed online during their lifetime,

whereas 3% reported being sexually harassed online within the past 12 months (ADL, 2023). Respondents from marginalized populations were more likely to report having been sexually harassed online during their lifetime (12%) compared to respondents from non-marginalized populations (5%).

Table 3: Image-Based Sexual Abuse Prevalence Estimates by Victim Group

Category	Type of IBSA	Prevalence Rate	Sample	Source
Adults	Distribution of sexually graphic images of individuals without their consent	12.8% 8% experienced IBSA 4.8% were threatened with IBSA	N=3,044 U.S. adults recruited through Facebook	Eaton et al., 2017 (Cyber Civil Rights Initiative, CCRI)
Adults	Images/videos publicly shared to the internet	1.1% (ever experienced)	N=873 Spanish adults	Gámez-Guadix et al., 2015
Adults/Adolescents	Having a sext forwarded/ distributed without consent	0.8% - 24.09% 8.78% average pooled effect size	Meta-analysis of 19 studies	Patel & Roesch, 2020
Adults/Adolescents	Revenge & nonconsensual pornography	8.3% (lifetime)	Systematic review of 82 studies	Walker & Sleath 2017
Adolescents	Images/videos publicly shared	1.5% (last 3 months	N=1,008 adolescents aged 14-19	Dick et al., 2014
Adolescents	Images/videos publicly and privately shared	32%	Adolescents that specified they participate in sexting	Stanley et al., 2018; Wood, Barter, Stanley, Aghtaie, & Larkins, 2015
College Students	Nonconsensual sharing of sexually explicit messages, pictures,	21.5%	N=391 Nationally representative	Walker et al., 2019

Category	Type of IBSA	Prevalence Rate	Sample	Source
	and videos		sample of UK college students	
College Students	Images/videos shared publicly or privately	6.3% (past 12 months)	N=540 college students aged 18-25	Marganski & Melander, 2018
College Students	Coerced sexting (sending of intimate images)	20%	N=480 college students	Drouin, Ross, & Tobin, 2015
Childhood (<18 years old)	Image-based sexual abuse (misuse of images; threats/pressure to obtain images; voluntarily provided images to older partner; and commercial talk, images, or other sexual activity)	11%	N=2,639 young adults (ages 18-28) asked about childhood experiences of online sexual offenses Nationally representative sample in the US	Finkelhor et al., 2022

Doxing

As discussed above, doxing research is most often found in the political, activist, and cybersecurity domains; few studies have examined doxing in an IPV context. Indeed, keyword searches in several criminal justice databases produced only three studies that included estimates of doxing victimization, two of which included samples outside of the U.S. These are shown in Table 4.

Sambasivan and colleagues (2019) conducted interviews and focus groups with 199 people who identified as women in three South Asian countries and reported that 14% had experienced doxing. Chen, Chan, and Cheung (2018) surveyed 2,120 secondary school students in Hong Kong. Their results showed that 31% of the students had experienced at least one type of doxing victimization. The most common types of doxed information among the sample were personal photos or videos (31%), name (30%), birthday (24%), mobile phone number (15%), and school name (15%). Finally, Kowert and Cook (2022) surveyed 377 gamers to examine "dark participation" in video games, including doxing. The authors reported that 11.1% of their sample had personally experienced doxing while playing online video games, and an additional 24.1% of the sample had witnessed the doxing of another gamer.

Findings from the Online Hate and Harassment survey conducted by the Anti-Defamation League (2022) provide some additional estimates related to doxing by victim

subgroups. Respondents were asked, "Had someone released private information about you, also known as doxing [ever or in the past 12 months]" (p.12). The survey also provided some additional language to indicate that doxing is "having personal information exposed, often for the purpose of further harassment." Approximately 5% of respondents indicated that they had been doxed in their lifetime; whereas around 3% of respondents indicated that they had been doxed in the past 12 months. The results were also disaggregated demographically. Six percent of respondents identified as being marginalized reported having been doxed in their lifetime compared to 4% of respondents from non-marginalized populations. There were no gender differences in the likelihood of reporting prior experiences of doxing (i.e., 5% males and 5% females). When the analyses were restricted to only those individuals who identified as LGBTQ+, the results revealed that approximately 23% indicated that they had experienced doxing and 13% had experienced doxing in the past 12 months.

Table 4: Doxing Prevalence Estimates by Victim Group

Category	Type of Doxing	Prevalence Rate	Sample	Source
Adults	Definition not given	11%	N=377 gamers recruited via Twitter and Facebook	Kowert and Cook, 2022
Adults	Releasing private information about a person; having personal information exposed, often for the purpose of further harassment	5% 3% 1-year rate	N= 2,300 adults Nationally representative sample	Anti-Defamation League, 2022
Adults	Non-consensual sharing of photos, conversations, and identity	14%	N=199 people who identified as women in India, Pakistan, and Bangladesh	Sambasivan et al., 2019
Adolescents	Intentional disclosure of private information about an individual on the Internet without his/her consent	31%	N=2,120 adolescents in Hong Kong	Chen et al., 2018

Limitations of TFA Prevalence Estimates

When examining the prevalence of victimization across crime types, it is important to note the limitations of these estimates. A longstanding body of research has indicated that crimes often go unreported, and this is particularly true for both TFA and "offline" intimate partner violence (Clevenger et al., 2018). In criminal justice research, this is known as the "dark figure

41

of crime" (Biderman & Reiss, 1967). For example, using data from the 2019 Supplemental Victimization Survey to the National Crime Victimization Survey (NCVS), Morgan and Truman (2022) found that although 67% of stalking victims knew their stalker, only 29% of all stalking victims reported their victimization to police. Similarly, Mumford et al. (2023) found that more than 70% of respondents who experienced TFA do not seek any help. Furthermore, individuals who experience TFA by a current or former intimate partner are less likely to seek help from law enforcement or the legal system compared to people victimized by an acquaintance or stranger.

Scholars have identified several potential reasons that contribute to differences in the reporting of crimes to law enforcement between traditional (i.e., face-to-face crimes) and cybercrimes (Graham et al., 2019). First, the harm inflicted on victims by TFA perpetrators does not have to converge in time and space as described in traditional routine activities theory (Cohen & Felson, 1979). The convergence occurs when the victim experiences the intent and effects of the act, which may occur at a time later than when the act was carried out by the perpetrator (Reyns et al., 2011; see also, Yar, 2005). Second, it can be difficult for victims and law enforcement to identify the perpetrator because their online identity could be fictitious or anonymous (Navarro & Jasinski, 2012). Lastly, law enforcement officers require specific training and or sophisticated knowledge of technology to gather evidence and effectively prove that a crime was committed in order to arrest a perpetrator. In some instances, law enforcement officers are not adequately trained, nor may they be willing to dedicate the resources necessary to handle the oftentimes complex nature of these offenses. They may also be less likely to take these crimes seriously and remain likely to engage in victim blaming as described elsewhere in this report.

Similarly, TFA prevalence estimates that rely on self-report surveys may underestimate its presence among domestic abuse survivors. According to Dragiewicz (2021),

> *Domestic violence survivors who know or suspect that their partner is monitoring their electronic communication or has unauthorized access to their online activities are perhaps the least likely to participate in surveys targeting community samples, meaning that the target population, abuse survivors, are likely excluded from surveys using community samples.*
>
> *Dragiewicz, 2021 p. 7*

In summary, studies have shown that there is considerable variation in the prevalence estimates related to TFA crimes. Differences are partly due to how these behaviors are defined as well as survey methodologies (e.g., sampling frame). Of the prevalence estimates described above, only a few conducted nationally representative surveys of the general population. National-level estimates reveal that approximately 1.3% of individuals ages 16 and over reported having experienced stalking involving technology (Morgan & Truman, 2022). A higher percentage of the population reported having experienced IBSA/NCP. CCRI conducted a nationally representative survey of adults and found that 12.8% of the sample reported having experienced some form of what we refer to as IBSA today (8% actual distribution of media and 4.8% threats of distribution). With respect to doxing, the Anti-Defamation League (2022) found that 5% of adults reported having been doxed in their lifetime, with 3% reporting that they were doxed within the past 12 months.

While these studies provide a snapshot of the prevalence of TFA in the general population, research indicates that TFA victimization may disproportionately impact subgroups of the general population (e.g., LGBTQ+, Non-Whites, females). Prevalence estimates are particularly important for calculating the costs associated with crime, given that they are the multiplier used with individual costs to construct national estimates. This has important implications for policy and practice.

Background on Estimation Methods for Costs of Crime

One of the uses of crime prevalence estimates is as an input to estimate the costs of crime and victimization. Specifically, the prevalence rate is the multiplier used with cost data to estimate the total cost of crime for the country, a state, or a city.

Cost estimation research for policy decision making, and the application of these methods to crime problems, has grown recently but its history is rich. To measure magnitudes of harm in dollar terms, early studies focused on tangible economic costs: those that can be directly measured and are usually out-of-pocket costs of victimization. In short, *tangible costs* are costs for which one can produce an invoice, such as medical bills and property losses. Estimating these is essentially an accounting exercise that tallies up known and paid costs; these are considered "bottom-up" methods of cost estimation (Lugo et al., 2018).

These estimates often miss critical costs, however, such as the portion of medical care paid by insurance or the lasting psychological trauma of victimization and its second-order impacts on things like work productivity and social functioning. Later work has made great strides in estimating these *intangible costs* as well, or those harms that are more difficult to quantify such as pain and suffering (Miller et al., 1996; Cohen, 2020). These estimations involve more "top-down" methods that seek to calculate total cost or valuation for a crime rather than simply summing known data on component parts. Several top-down methods have been developed over the years: *stated preference* methods where an individual states an amount they would be willing to pay to address the problem; *revealed preference* models that assess market-based information on how much individuals are willing to pay to avoid victimization; and analysis of the values that juries place on various victimizations in their *jury award* decisions. These methods are discussed in more detail below.

Regardless of the approach used, cost of crime estimates are undertaken to allow decision makers to make comparisons along a common metric, such as comparing amounts of harm caused by different crimes, comparing the crime problem to other social problems, or comparing the costs imposed by the occurrence of crime to the costs of efforts to prevent it (Government Accountability Office, 2017; Lugo et al., 2018).

While victimization cost estimates can be used to answer a variety of important policy questions, the most common purpose for which they are used is to inform the effective allocation of finite public resources by government (Cohen, 2020). Information on costs, and from cost-benefit analyses of different programmatic solutions, is critical for this kind of decision making. Policy makers must have some way to compare programs' effectiveness in reducing various problems to decide which should receive public funding, and how much (Stokey & Zeckhauser, 1978). An argument can be made that each time a crime reduction or victim assistance policy or program is implemented, the harms of crime are inherently monetized.

The current push for evidence-based policy has elevated the need for information about which policies and programs reduce crime victimization incidence and harms the most, for the lowest cost (Hunink et al., 2001). Furthermore, while estimates of the cost of all crime

victimization are useful for some purposes, crime type-specific costs are also needed to understand the extent of need, especially for emerging crime types such as TFA.

While progress has been made in estimating total costs of victimization more accurately, there are still gaps. Importantly, many studies have neglected to map the unequal distribution of harms and costs by race or ethnicity, age, sexual orientation, disability, income, or geographic location; harms are not experienced equally and in the same way by all groups (McLean & Bocinski, 2017). For example, Chalfin (2015) estimated the cost of all crime to be approximately $200 billion per year by using the 2012 index crime counts from the FBI's Uniform Crime Reports (UCR). However, when including estimates of the costs of unreported crimes, Chalfin estimates that the cost may be as high as $310 billion and still fails to account for variance in responses of individuals to crime and to changes in crime rates. A focus on solely street crime and felonies via the UCR further hinders cost estimates as the high costs of misdemeanor and white-collar offenses are excluded (Raskolnikov, 2020).

Failing to account for all relevant offenses when trying to estimate the total cost of all crime—or failing to map the unequal distribution or experiences of harm across various population groups—can lead to an inefficient allocation of resources to reduce the problem. This study attempts to include disaggregation of TFA harms across different sub-populations to inform decision-making to address these emerging and evolving victimization types. However, first we present a brief review of the major cost estimation methods (see Lugo et al., 2018 for a thorough evaluation of the full range of methods). We then explain the reasoning for the methodology chosen in this study.

Methods for Cost Analysis

Top-down and bottom-up methods are two categories of methods for measuring the costs of crime. Bottom-up techniques measure the discrete and tangible financial costs of crime, such as medical expenditures, property losses, law enforcement costs (time, resources), and loss of employment (lost income, job search costs) (Lugo, et al., 2018). However, applications of bottom-up methods are often limited to broader crime categories (e.g., property crime, homicide) because it is more difficult to disaggregate within these categories using standard federal crime data. Furthermore, bottom-up methods cannot easily capture the costs of intangible harms such as fear or lost quality of life. Finally, bottom-up methods generally capture costs to individual victims and not to the public at large who might be concerned about the risk of victimization for themselves, their families, or friends.

To account for these other intangible or indirect costs, experts have recommended the use of top-down techniques such as those mentioned above. With top-down measures of costs, intangible costs can be measured by determining individual perceived burdens of costs – determined either by their market-based actions (e.g., wage rates for risky jobs, purchasing of security alarms or guard dogs, home prices in high crime vs. low crime areas—*revealed preference*) or through the use of surveys in which individuals are asked to state their willingness to pay (WTP) to avoid or reduce victimization or its harms (*stated preference*).

Economists generally prefer revealed preference data if available, but it is often difficult to isolate crime avoidance-related costs because few market-based decisions, like home purchases, involve consideration of only one factor. Revealed preference choices are further limited by the individual's ability to pay (Cohen, 2020: Chapter 7); someone may deeply value the opportunity to move to a safer neighborhood but be unable to afford it. It is also difficult to identify the crime component of many such decisions. For example, a guard dog might provide companionship as well as security, and a risky job is likely to have other amenities and disamenities – likely correlated with risk (e.g., the taxicab driver who runs the risk of being robbed but likes to be out and about and enjoys the flexible schedule).

Alternatively, stated preference/WTP surveys can be tailored to ask about individual crime types without this joint production problem. They can also value crimes that are not affected as much by market-based prevention activities and can include responses from a nationally representative sample; this allows disaggregation by crime type, the ability to analyze harm valuation by different population groups, and to ask about targeted policy preferences of interest (e.g., Cohen & Bowles, 2010; Lugo et al., 2018).

Willingness to Pay Models

Willingness to pay (WTP) studies are an established method for estimating holistic (tangible and intangible) costs to society associated with victimization (Ludwig & Cook, 2001; Cohen et al., 2004; Piquero et al., 2011; Lugo et al., 2018). By collecting information on the amount an individual is willing to pay to avoid the negative impacts of crime victimization, Cohen (2020) explains that willingness-to-pay (WTP) methods address questions related to the economic valuation of policies and programs for crime prevention by answering "how much the public expects to benefit…[and] how much they would be willing to pay for the program" (p. 164). These are *ex ante* valuations: how much the individual would pay to prevent the crime *before* it occurs.

WTP questions are frequently asked directly of individuals at-risk of victimization and/or of the general public in survey research, focus groups, and interviews. A common WTP question will ask respondents if they would approve of programs which reduce a specific crime by some percentage but would cost them a specific dollar amount. The percentage reductions of crime and the cost of the program are varied to gauge the elasticity of demand for investment in reducing that crime (Lugo, et al., 2018). This information is then combined with some measure of prevalence to generate a per-victimization cost estimate (Arrow et al., 1993; Cohen et al., 2004; Cohen & Piquero, 2009).

WTP methods are not without challenges. First, they are based on responses to hypothetical questions, not actual market transactions. Second, WTP methods have several methodological issues. A respondent's willingness to pay can also be affected by things like political views on taxes, their income/ability to pay, their ability to understand and answer questions involving hypotheticals, and their ability to assess their level of risk. As a result, these respondents' perception of risks and costs do not necessarily represent the average individual (Dominguez & Raphael, 2015). It is generally accepted practice to ask separate questions that

allow researchers to control for at least some of these other factors that can influence responses (Ludwig & Cook, 2001). Relatedly, a respondent with a high general fear of crime may prefer to spend a larger share to avoid becoming a victim (Cohen, 2020, p. 131). In some situations, fear of crime can be measured and accounted for while in others it is difficult, if not impossible, to accurately quantify it (Cohen, 2020).

Another critique of WTP measures is that they are unable to tease out the costs related to preventing pain and suffering versus costs related to preventing reductions in quality of life (Cohen, 2020). Quality of life, as opposed to pain and suffering, refers to the monetization of losses associated with things like no longer being able to enjoy activities that one used to do. Cohen (2020) argues that these concepts are different and that a respondent's assessment of risk associated with each of these can affect their willingness-to-pay for reductions in these risks. These differences are conceptually simple to understand, but almost impossible to tease out empirically (Cohen, 2020, p. 39).

Fortunately, this is not necessary to estimate *total* willingness to pay. Next, two of the main WTP methodologies are presented: contingent valuation and discrete choice experiments.

Contingent Valuation. Contingent valuation (CV) methods were originally used to value non-market amenities and disamenities such as clean air or the loss of endangered species—things that are not generally traded in the marketplace but are affected by it. For example, CV methods were used widely to attempt valuation of the damage from the Exxon Valdez and BP Deepwater Horizon oil spills, going beyond pure financial losses such as reduced tourism or property damage to include the intangible value of natural resources (Kling et al., 2012).

In 1993, economists Arrow and Solow convened an expert panel of other economists that endorsed the general CV method and recommended various "best practices" at the time. For example, they concluded that open-ended questions asking respondents to indicate a dollar amount of their willingness-to-pay for non-market goods and amenities may bias responses upward by incorporating an overall "warm glow" effect associated with the particular amenity or disamenity in question rather than the respondent's actual valuation of that good. The concern is that respondents might provide their assessment of dislike of a harm in general and not for a specific level of harm. For example, a respondent who dislikes "crime" might assign the same value to a reduction of 10% and a reduction of 30% instead of focusing on the level of crime reduction value itself (Lee & Fisher, 2020).

Discrete Choice Experiments. Discrete Choice Experiments (DCEs) are a more sophisticated form of contingent valuation that economists now recommend that overcomes some of the limitations of CV surveys (Tinelli, 2016; Cohen, 2020). The DCE method of obtaining WTP estimates is also commonly used to value environmental amenities and is the state-of-the-art approach generally preferred by experts in WTP methodology (Louviere et al., 2000).

DCEs provide respondents with a choice between a set of crime reductions and costs – sometimes also varying competing policies or programs. Unlike some of the earlier approaches, a DCE does not directly elicit a dollar valuation. Instead, it provides two or more alternative

"bundles" of costs and benefits and asks respondents to select one (e.g., Picasso and Cohen, 2019). In these questions the percentage reductions in crime or victimization are varied along with the costs for each program (e.g., Tinelli, 2016). Respondents are then asked to select which bundle of crimes and costs (and potentially programs) they would prefer. This allows respondents to view distinct choice sets and their selections permits researchers to identify the individual value of each component of the bundle (Cohen, 2020; Tinelli, 2016; Louviere, Hensher & Swait, 2000). In more simplistic DCEs, the program outcome remains the same while the costs are varied (Lugo et al., 2018). However, more recent DCEs vary not only the costs but also the outcomes (Cohen, 2020). While more complex, such questions provide researchers with insight into the combinatory valuations of both reductions and costs.

Box 1 shows a hypothetical example of a discrete choice question using robbery. While the context is different, the format of this example is based on prior DCE studies. In this example, respondents are provided with a definition of robbery, common victim consequences, and estimates of the prevalence of this offense. Note that the prevalence estimate used in a DCE question does not have to be exact—only within an order of magnitude of actual prevalence rates—because the purpose of the DCE is to value marginal changes in prevalence.

Note that in this example, we have included another parameter: a policy choice. For example, the 25% reduction is based on increased street lighting and patrol, the 50% reduction is based on increased punishment of offenders, and the 75% reduction includes the implementation of both policies. The order of policies can be further randomized so that half of respondents are told that victim assistance will provide a 25% reduction while the other half are told that increased incapacitation provides a 25% reduction. Other randomizations could also be added to this framework depending on the focus of the study.

By including a "price" in the description of the bundle of remedies, either through a voluntary contribution or a tax, researchers can infer the marginal willingness to pay for different components of bundles of policies and reductions in crime. This method is more realistic in that it involves trade-offs instead of open-ended questions that are subject to gaming and speculation by respondents. It also overcomes many of the limitations of other survey methods of eliciting willingness-to-pay by allowing for within-person "scope tests" (i.e., determining whether respondent valuations vary with the frequency of the offense) and testing whether a respondent's valuation depends upon the policy choice for reducing crime (see Carson and Louviere, 2017 and Picasso and Cohen, 2019). The DCE method also incorporates a clear "status quo" option as well as the ability to vary remedies to provide a more meaningful and nuanced estimate of costs.

Box 1. Hypothetical Discrete Choice Experiment Question

We would like to ask you about your views of the problem of robbery in your state. There are no "right" or "wrong" answers – your opinion is all that matters.

We will be asking you to choose between different options that reduce the number of victimizations or the harm caused by robbery. All of these programs require additional money to implement and would require either raising taxes or reducing other services. We want you to think about the proposed programs and assume they have been shown to reduce crime. We also want you to answer each question as if you actually would have to pay the amount you enter. However, one option will always be the status quo – in other words, you can choose to pay nothing and implement no new crime reduction program.

Background Information Provided to Respondents:
Robbery – Definition
The FBI defines robbery as the taking or attempting to take anything of value from the care, custody, or control of a person or persons by force or threat of force or violence and/or by putting the victim in fear.

Annual Victimization in U.S.
• About 20 million robbery victims in the U.S.
• About 100 out of every 1,000 (10%) U.S. adults

Victim harms can include legal and insurance costs, costs to replace the property lost, medical and mental health costs to deal with trauma if the property was taken by force, etc.

Survey Question:
Your state government is considering the following new **robbery** reduction programs proven to be successful in other states. *[Note: The order of Options A and B are randomly assigned.]*
Option A – Increased street lighting and patrol to prevent future robberies.
Option B – Increased punishment for offenders.

	Option A	Option B	Option C	Option D
Reduction in Robbery	Reduced by 25% (from 100 per 1,000 to 75 per 1,000)	Reduced by 50% (from 100 per 1,000 to 50 per 1,000)	Reduced by 75% (from 100 per 1,000 to 25 per 1,000)	None
Policy	Increased street lighting and patrol to prevent future robberies.	Increased punishment for offenders.	Both policies A and B.	No new policies.
Annual cost per household	*$50 / $100**	*$100 / $200**	*$200 / $400**	No Cost

* Note: dollar amounts are randomly assigned.

Strengths and Weaknesses of DCEs

DCEs do face some of the same challenges as other cost estimates using survey approaches. First, there is the potential for overestimating costs of crime due to asking respondents to express hypothetical preferences rather than observing actual activity in which resources may be limited and actual risks are present (Rakotonarivo et al., 2016; Maurer et al., 2017). Further, arguments about the inability to directly measure intangible costs can lead some researchers to conflate them with tangible costs and create a single cost estimate that adds the willingness-to-pay estimates with tangible costs (Clear & Austin, 2021). One can argue, however, that combining estimates of total costs using a top-down method with other data on tangible costs from "bottom-up" methods can be used to calculate the portion of total cost that come from intangible costs (to simplify, Total Cost from DCE – Tangible Costs = Intangible Costs).

Other general critiques of DCEs concern the reliability and validity of the estimates they produce. In a systematic review of 87 DCE studies valuing non-market environmental goods, Rakotonarivo et al. (2016) argue that estimate reliability can be affected by minor changes in survey design. Their review showed that different levels of complexity in the choice sets changed choice outcomes: when choice sets, alternatives, attributes, and levels ("bundles") increased in complexity, reliability tests of the data appeared to reflect a struggle among respondents to make meaningful differentiations and valuations between them (see also Clear & Austin, 2021; Tinelli, 2016). Studies have long shown that changes in wording, question order, and other seemingly minor components of survey design can impact results (Schuman & Presser, 1981). However, survey design complexities such as these can be dealt with using sophisticated design principals, employing skilled methodologists, and employing multiple waves of cognitive testing and pretesting of the survey prior to deployment.

Due to the flexibility offered by this approach, DCEs have become the preferred method of contingent valuation and willingness-to-pay cost estimation (Cohen & Farrington, 2021). Furthermore, Picasso & Cohen (2019) point out that benefits of DCEs include its ability to compare various policies, risks, and payment levels within the same respondent. This means that DCEs allow for "scope tests" within subjects (Cohen et al., 2021; Lugo et al., 2019). A scope test confirms monotonic preferences among respondents. Monotonicity is a core assumption for valuation of preferences in economics (Debreu, 1964). With monotonic preferences, a respondent would prefer to pay more for a greater reduction in crime. However, certain situations can affect such preferences. As a result, DCEs provide insight into respondents' conceptualization of risk and effectiveness. Additionally, DCEs measure how individuals make "trade-offs" in attributes of programs or policies that are important to them (Tinelli, 2016; Raskolnikov, 2020). These assessments are critical in accurately measuring the cost of crime beyond market valuations such as property losses alone (Blythe et al., 2020).

Key Takeaways: Cost Estimation Methods

Researchers in various fields have continuously worked for decades to develop accurate ways to estimate economic costs of social phenomena, including costs-of-crime (Cohen, 2020).

Economists have developed methods ranging from measuring tangible costs by simply summing up the "receipts" from various out of pocket costs to various methods of asking respondents their willingness-to-pay for specific reductions in crime or for prevention and treatment programs (CV, DCEs) and using those to calculate a total cost of crime. In more recent years, discrete choice experiments have become the preferred method for estimating total costs because of the great flexibility and benefits they offer when constructed thoughtfully and rigorously. They represent the current state-of-the-art in top-down cost estimation. In this study, the nationally representative survey uses DCEs along with questions on victimization experiences and tangible harms suffered to generate estimates of a variety of TFA victimization costs that can be disaggregated by victim group, thus also enabling some delineation of the uneven distribution of harms between different groups as well as differences in their stated preferences.

Taxonomy of Harms

One of the main contributions of this research is a taxonomy enumerating and classifying the costs and harms that three types of TFA – cyberstalking, IBSA, and doxing – cause for victims and, secondarily, for society. For these purposes, the term "costs" is used for items for which dollar figures would be assigned, and "harms" refers to more general consequences that are not so easily measured. The taxonomy is summarized in Table 5 and described below. The authors developed this taxonomy by integrating input from the literature review, the SME interviews, and the Advisory Board discussions, and iterative consultation with project partners. The input from each of these sources is synthesized in the descriptions that follow.

One of the big takeaways from our interviews and consultative meetings was that most types of costs and harms were experienced by victims across all three TFA types. The table also shows who we anticipate would typically pay the majority of costs associated with the various harms on a general basis (e.g., victim, victim service providers that can include government and private sources, employers, friends and family, society in general). Table 5 reflects this general approach, though there are some costs and harms that were experienced more often, more severely, or differently by certain victim/survivor groups. These disproportionate experiences of harm are discussed after the general taxonomy is presented.

This taxonomy does not re-invent the wheel. Rather, it starts from the work of Mark Cohen and colleagues (Cohen et al., 1994; Miller et al., 1996; GAO, 2017). Previous research estimating the costs and harms associated with crime victimization has typically categorized these losses as tangible (e.g., the value of household goods stolen during a burglary or the cost of medical appointments—things for which one might have a receipt) and intangible costs such as pain and suffering, which are more difficult to quantify (e.g., Miller et al., 1993; Miller et al., 1996; Cohen, 2020).

Consistent with previous research, this taxonomy is therefore organized in two levels. First, costs are split into the two categories of tangible/direct costs and more intangible/indirect harms. Then, within the tangible and intangible categories, costs and harms are further organized by subcategory. Some costs and harms can arguably contain both tangible and intangible components; i.e., a physical injury can result in a tangible cost that has a receipt (medical treatment) and an intangible harm (lost quality of life). Each harm was categorized according to its dominant characteristic if the component parts could not be easily broken out.

This section of the report presents the final taxonomy and the evidence supporting the inclusion and categorization of each cost and harm, beginning with tangible costs. The table addresses broad categories while the details are provided in text.

Tangible Costs

The tangible financial costs identified in this taxonomy and presented in Table 5 fall into the following groupings: productivity costs, education costs, medical costs, property costs, social

presence costs, legal costs, and other financial costs.

Productivity Costs. Productivity costs include harms related to lost wages from attending court or needing time off for various reasons (McLean & Bocinski 2017; Wolak et al., 2017), reduced productivity on the job (Cohen 2020; Fissel & Reyns, 2020; McGlynn et al., 2021), loss of employment or job altogether (Cheyne & Guggisberg, 2018; Bates 2017), and the costs of new employer-provided protections, such as technology and safety checks and trainings, that are instituted as the result of an employee's victimization (SME Interviews). Costs for time off may be borne by the employee if paid or the employee if unpaid.

Job loss can manifest a number of ways. For example, someone who is fired from a job might not qualify for unemployment, could lose a professional license, and might not easily secure references for a new position. This is different from someone who quits, who could potentially secure references and employment more readily down the line, or from someone who is "terminated" and is found eligible to receive unemployment (Advisory Board).

Victims of all three forms of TFA included in this study often suffer lost productivity, which costs both the victim and the employer. Reduced productivity and job loss have been reported by victims of cyberstalking due to constant intrusions from the perpetrator, which sometimes carry over into the workplace (Cheyne & Guggisberg, 2018). IBSA victims have reported the loss of entire careers when their reputations are ruined (Bates, 2017). Even when job loss is avoided, IBSA victims can lose productivity from repeatedly checking the internet for their photos during work hours, stigma from coworkers, and the resulting inability to concentrate (McGlynn et al., 2021). IBSA and doxing victims additionally reported closing online business accounts and blogs which led to the loss of jobs and career opportunities (Citron & Franks, 2014).

Education Costs. Cyberstalking victims report education-related consequences resulting from their victimization that include poorer performance during class, on assignments, or during exams; missed deadlines, assignments, or exams; high absenteeism; dropped classes; lower grades; and failed classes (Fissel & Reyns, 2020; Advisory Board Discussions). Educational consequences are experienced by victims of many types of abuse (Cohen, 2020), including TFA, as they contend with shame, social pressure, physical and mental health effects, and other intangible harms discussed below that lead to these tangible costs. These interrelated harms can impact school enrollment and success and create tangible costs related to transferring schools or dropping out such as lost tuition money, additional school application fees, and costs of moving or changing living situations (e.g., costs associated with moving out of dorms or in with family or friends; Advisory Board Discussions). Furthermore, victims may attain lower lifetime wages as a result of diminished educational attainment (McLean & Bocinski 2017; Wolak et al., 2017).

Physical/Mental Health Costs. Victims of all forms of TFA suffer a range of mental, physical, and emotional health effects, all of which can necessitate costly treatment to support victim recovery (McLean & Bocinski 2017; Wolak et al., 2017; Cheyne & Guggisberg, 2018; SME Interviews). These interrelated health impacts that have both tangible and intangible components are discussed together, with the focus in this section on the medical bills they generate. Their impacts on quality of life are discussed under intangible harms.

Reported impacts requiring medical and/or mental health treatment, which is usually paid by a combination of insurance, victim assistance or compensation, and out of pocket costs, include post-traumatic stress disorder (PTSD); anxiety; mood disorders; panic disorders, depression; paranoia; phobias; suicidal thoughts; losses of self-esteem, confidence, control, and sleep; nightmares; and increased alcohol and drug use (Bates 2017; Cheyne & Guggisberg, 2018; Fissel & Reyns, 2020). Minor victims have additionally manifested aggressiveness, hostility, and risky behavior in offline situations. Minor girls with recent cyber abuse victimization experience, when compared to girls who had not experience cyber abuse, were two to four times more likely not to use any form of contraception and three to six times more likely to have recently experienced reproductive coercion (Dick et al., 2014). Tangible costs related to these can include mental health therapy, prescription medications, and early parenthood, among others.

Physical manifestations, many requiring medical treatment, can include weight change, change in appetite, sleep disorders, headaches, tiredness, stomach aches, nausea, weakness, self-harm, laxative use, and forced vomiting (Begotti & Acquadro Maran, 2019; Fissel & Reyns, 2020). Recent estimates indicate that nearly one in six people (17%) ages 18 to 35 who experience TFA are also physically harmed by the same abuser (NORC, 2022). If the online abuse escalates into offline abuse by the perpetrator or others the abuser has instigated, physical consequences requiring medical care can also include bruising, bleeding, broken bones, pregnancy, sexually transmitted infections, and so on (Advisory Board).

All of these mental, emotional, and physical health harms create tangible treatment-related costs and additional costs related to their impacts on work, school, home, and social situations.

Property Costs. TFA can result in fees and costs related to breaking technology service contracts and setting up new services; purchasing new devices and computers, new security systems, tracking services, forensic software to locate evidence; property destruction from abuse that moves offline; and even expenses related to housing instability or relocation if the victim must move as a result of the abuse (Lee & Anderson 2016; McLean & Bocinski 2017; Wolak et al., 2017; Cheyne & Guggisberg, 2018; Anti-Defamation League 2019; Cohen 2020; Truman & Morgan 2021; Turgoose et al., 2021).

Social Presence Costs. With the ubiquity of online management for banking, shopping, watching television, "smart home" feature control, and most aspects of day-to-day life, changing online behaviors to avoid an abuser takes significant time, skill, and money (Anti-Defamation League 2019; Grimani, et al., 2020; Lee & Anderson 2016; Matthews et al., 2017). In addition to restructuring one's entire financial life, victims often must pay for services to remove content from the internet such as DeleteMe, safety trainings, monitoring services, and identity restoration/protection services to extricate themselves from the abuser's control (Advisory Board Discussions). This process can leave a victim/survivor with reduced ability to access services, banking, bill pay, and other activities if they live in continued fear of being "found" online by their abuser. In turn, these reduced abilities can lead to further unexpected time and financial costs to conduct day-to-day life activities (SME Interviews).

Legal Costs. Dealing with TFA can incur a number of legal costs including time and money to pursue legal options in tort law (financial, property and housing issues), copyright law (ownership of images), criminal law (prosecutions and victims' rights), privacy rights enforcement, and navigating free speech exceptions in online conduct (Benedick, 2017; Cheyne & Guggisberg, 2018; SME Interviews). IBSA involving minor victims can result in additional legal defense costs if child pornography charges are levied on the victim reporting the crime: lack of education about IBSA-related laws and how to handle IBSA cases means that a minor who sends explicit images of themselves to someone else may be charged with distributing child pornography—even though they are the victim and the pictures are of themselves (Wolak, Janis, & Finkelhor, 2017).

Other Direct Financial Costs. Several other tangible costs can also result from TFA victimization. These can include risk-reduction costs (Cohen, 2020) such as paying for self-defense classes (Anti-Defamation League, 2019). Resolving TFA-related financial problems can include expenses to deal with debt and repair credit and credit histories (McLean & Bocinski 2017; Wolak et al., 2017). Ruined credit resulting from cyberstalkers' interference with financial accounts or debt incurred after job loss can also reduce future access to loans, jobs, and housing if not repaired—all time-consuming and costly processes (Clevenger & Navarro, 2021). IBSA survivors have even reported sustained financial ruin after their images were shared and reshared again long after they thought all images were removed (Bates, 2017; Advisory Board Discussions). Financial and reputational repair can be a long and arduous process, especially when so many still blame victims of TFA for their abuse.

Intangible Harms

Intangible harms or costs are those that are more difficult to place a financial value on because there is not necessarily an invoice with a record of the total cost. However, there are some methods for calculating these, as discussed in the section of the literature review covering the crime cost estimation literature. The national survey which we conduct in the second phase of this project will be used to estimate some of these costs for TFA.

Table 5: Taxonomy of Harms and Costs of IPV-Related TFA

Harms/Costs of Cyberstalking, IBSA, and Doxing			Who Pays?
Direct Financial Costs (Tangible Costs)	**Productivity costs**	Lost wages (attending court; unpaid time off)	Victim
		Loss of employment	Victim
		Loss of productivity on the job	Victim, Employers
		New technology and safety trainings and checks	Employers
	Education costs	Missed school days	Victim
		Decreased school performance	Victim
		Costs/fees associated with changing schools	Victim

Harms/Costs of Cyberstalking, IBSA, and Doxing			Who Pays?
		Dropout of school (lost tuition/fees)	Victim
		Reduced lifetime income as a result of dropping out	Victim
	Medical costs	Physical health treatment costs (e.g., co-pays, out-of-pocket expenses, deductibles, prescriptions)	Victim, Vic. Svcs., Health Insurance
		Mental health treatment costs (e.g., therapy; medications)	Victim, Vic. Svcs., Health Insurance
	Property costs	Costs related to technology service providers (broken contracts; new services) to prevent future victimization	Victim
		Costs related to changes in technology (new devices) to prevent future victimization	Victim
		Home security monitors and alarm systems	Victim
		Destruction of property	Victim
		Relocation	Victim
	Social presence financial costs	Content monitoring/ removal services	Victim
		Online/offline safety trainings	Victim, Employer, Vic Svcs.
		Services to monitor internet activity	Victim
		Identity services (changing identity)	Victim
	Legal financial costs	Attorney fees (private)	Victim
		Court costs/fees	Victim, Vic Svcs.
	Other financial costs	Loss of credit and expenses of repairing it	Victim
		Changing bank accounts/credit cards, etc.	Victim
Intangible Harms & Costs	**Time costs (hours spent)**	Attendance at court, meeting with attorneys, obtaining other legal services, copying/filing legal documentation	Victim, Vic Svcs.
		Regaining control of/unlinking accounts	Victim
		Getting out of contracts, replacing devices, updating settings/ passwords	Victim
		Damage control: explaining what happened to others	Victim
		Searching for new employment	Victim
		Finding/obtaining medical/mental health services	Victim, Vic Svcs.

Harms/Costs of Cyberstalking, IBSA, and Doxing			Who Pays?
		Monitoring social media, internet, and other applications for abusive content, reporting the perpetrator's account to the tech platform, and requesting takedown of content	Victim
		Inability to focus on daily life activities (work; errands)	Victim
	Personal costs	Loss of personal freedom	Victim
		Lost feelings of safety	Victim
		Escalation (fatal violence, in-person physical harm)	Victim
		Being blamed for what happened	Victim
		Personal reputation	Victim
		Professional reputation/ Employment discrimination	Victim
		Housing discrimination	Victim
	Harms to mental health effects/ emotional well-being in addition to financial costs of treatment	Body dysmorphic disorder	Victim
		Shame/humiliation	Victim
		Trauma (PTSD; somatic symptoms)	Victim
		Substance abuse	Victim
		Self-harm	Victim
		Feelings of isolation	Victim
		Mistrust of others (personal; justice system)	Victim
		Hypervigilance (paranoia)	Victim
		Re-traumatization in legal, work, medical, family, and other settings	Victim
		Lasting physical harms (if abuse escalates offline)	Victim
		Loss of productivity, efficiency, passion	Victim
	Online personal behavioral changes	Cessation of use of technology	Victim
		Changes in interactions with technology	Victim
		Adverse reactions to technology	Victim
		Self-censorship (freedom of speech)	Victim
Intangible Harms & Costs (Continued)	**Offline personal freedom infringement**	Social isolation (Avoid going out in public; avoid family/friends/acquaintances)	Victim
		Loss of movement (feeling trapped; hiding)	Victim
		Loss of identity (e.g., changing name)	Victim
		Loss of support network	Victim
	Social costs to society	Elimination from work/civic activity	Society
		Sexualization of minors	Society
		Demeaning marginalized communities	Society

Harms/Costs of Cyberstalking, IBSA, and Doxing			Who Pays?
		Changes in personal relationships	Victim, Friends, Family, Employers
		Impact on secondary survivors (children; family; friends)	Friends, Family, Employers
		Society response to crime	Society
		Replacing employees	Employers
		Replacing tenants	Society, Landlords
		Economic costs and lost skills when victims leave the labor force	Society

Time. An enormous cost category of TFA is time spent by the victim and victim service providers to deal with and recover from the effects of the abuse. In some cases, employers, families, and others may also have time costs involved with addressing the harms of someone's victimization. There are methods to calculate time costs if the true number of hours spent can be documented, but it is not an exact science as estimates of time spent over weeks and years are usually approximate at best.

Nevertheless, there are costs in time associated with a wide array of activities such as reporting the abuse to digital platforms and/or police; proving the abuse (being one's own investigator); changing behaviors to protect privacy and security; obtaining legal services; attendance at criminal prosecution, sentencing, and release hearings; civil court proceedings; meeting with attorneys; and copying and filing documentation for courts and legal services (SME Interviews; Advisory Board Discussions). Additional time may be spent to regain control of and unlinking accounts, getting out of contracts, replacing devices, updating settings and passwords, and doing "damage control" explaining what happened to others (SME Interviews; Advisory Board Discussions). Time is spent avoiding abusers and future or continued victimization can include changing commutes, moving, avoiding being alone, or avoiding certain locations (Anti-Defamation League 2019; Turgoose et al. 2021). Searching for new employment, finding and obtaining medical and mental health services, monitoring social media and the internet for activity, and delays in completing daily tasks such as work, household responsibilities, social activities, or running errands due to trauma-induced inability to focus can also result in significant costs in time (Gavine, & Moncur 2020; Truman & Morgan 2021; Anti-Defamation League 2019; Lee & Anderson 2016; SME Interviews, Advisory Board Discussions).

Personal Costs. Several different intangible harms fall under the category of "personal costs." These additional harms that curtail daily activities or future opportunities largely center around the concept of isolation. These include loss of personal freedom to move about freely, lost feelings of safety, fear of revictimization, suffering blame for what happened, damage to

personal and professional reputations that can lead to employment or housing discrimination, and escalation of abuse offline into physical harm or even fatal violence (McGlynn et al., 2021; SME Interviews; Advisory Board Discussions).

According to McGlynn and colleagues (2021), IBSA victims particularly described a "totality of harm" that they experienced, or a cumulative result of the individual harms interacting with one another in their lives. This total experience can include:

- *social rupture* (e.g., disrupted lives; altered sense of self, identity, and relationships);
- the *impacts of isolation* on daily activities (e.g., distrust of people, especially men); distrust in all internet interactions (a "necessary evil");
- coping with *"existential threat"* and *feeling "trapped"* through hypervigilance and constantly assessing others' knowledge and opinions of them; and
- *constrained liberty* (e.g., sexualized images in ads cause retraumatization and feelings of living in a "narrowed down world"). (SME Interviews; see also McGlynn et al., 2021).

Women in Gosse's 2021 study of cyberabuse described their resulting isolation in terms of not wanting to tell people about abuse because previous advice discounted their experience; it was emotionally taxing to explain and seek validation, only to be told "it's not real." Women in this sample stated that not being taken seriously reduced their likelihood of seeking help in the future (Gosse, 2021).

Mental Health and Emotional Wellbeing. TFA victims suffer harms to mental and emotional health above and beyond the tangible costs of treatment described above. These mental and emotional effects are more difficult to quantify. While some, such as "fear, insecurity, intrusion, isolation, disbelief, confusion, guilt and shame" (Afrouz, 2021) are mentioned elsewhere in terms of their impacts on various activities and on financial health, this category is concerned with the direct effects of TFA on mental and emotional health on the victim generally.

Research has shown an association between all types of IPV-related offline and online abuse and depressive symptoms, such as feeling down or hopeless, annoyed and/or angry and loss of interest (Barter & Stanley 2016; Truman & Morgan 2021). IPV-related TFA has resulted in depression, insecurity, anxiety, fears for safety and privacy, grief, lower self-esteem, PTSD, panic attacks, distrust of others, sleep disturbances, and hypervigilance that can negatively impact well-being and social behaviors (Cheyne & Guggisberg, 2018; Begotti & Acquadro Maran, 2019; Klettke et al., 2019; Levy & Schneier, 2020; Afrouz, 2021; Gosse, 2021; SME Interviews). Minors fear particular social consequences for reporting, such as being shunned for getting the offender in trouble (Marques 2021) and a threatened sense of marginalization and exclusion from peers (Brion-Meisels & Garnett 2017).

Cantu and Charak (2022) conducted a survey with 902 college-going Hispanic emerging adults and found that depression increases with the occurrence of multiple concurrent forms of IPV-related TFA, indicating an additive impact of harms for polyvictims. In fact, unwanted cyber pursuit behaviors were even more strongly associated with PTSD and depressive

symptoms than in-person unwanted pursuit behaviors and physical, sexual, and psychological IPV (Dardis et al., 2018)—especially when the TFA is ongoing (Gini et al., 2018; Kuklytė 2018; Begotti & Acquadro Maran, 2019).

IBSA victims in Bates (2017) developed trust issues, obsessive and hypervigilant behavior, fear/anxiety leading to avoidance behavior, and negative self-image while also suffering public shame and humiliation, harassment, and/or stalking by others. Victims can experience ongoing intrusive thoughts and become caught in a state of "permanent remembering" (Mayer-Schönberger, 2009; Gini et al., 2018; Afrouz, 2021) in which they are unable to leave the past behind (Marques 2021; McGlynn et al., 2019). Others developed higher levels of psychological distress when *threatened* with the distribution of an image, including fears for their safety (Henry et al 2018).

Personal Behavioral Restrictions (Online and Offline). The emotional and mental toll of TFA, combined with new safety precautions undertaken, can result in victims and survivors severely curtailing their online presence and use of online services. Experiencing TFA can lead survivors to believe that all technology is "infected" or not to be trusted (Henry et al., 2019; see also Stevens et al., 2021). For example, even app notifications on one's cell phone or other devices can cause a victim to have a trauma response (Advisory Board Discussions).

With a dominant share of business now conducted over the Internet, these online behavioral changes come at a cost in today's connected world (Advisory Board Discussions). Many people's jobs, social lives, and public services access depend on an online presence (Homchick, 2019). Abuse limits that access when victims change contact information, remove online accounts, self-censor posts, stop using social media, or stop using a smartphone (Anti-Defamation League 2019; Grimani et al., 2020; Lenhart et al., 2016b; Vakhitova et al., 2019). Cyberstalking may cause victims to fear for their safety or the safety of others they know, including fear that perpetrators will harm pets or property (Truman & Morgan 2021). Doxing, especially when combining contact information with IBSA, can result in strangers soliciting victims for sex which additionally contributes to anxiety, lack of safety, and the emotional burden of dealing with unwanted contact and continual reminders (Citron & Franks, 2014). The loss of access after withdrawing from technology use then results in reduced ability to be "full participants in society and the digital world" (Bailey & Mathen 2017).

Restrictions in online behaviors often continue into offline activities, contributing to curtailed freedom of movement and participation in the rest of society as well. The victim may feel burdened to reduce safety risks by taking such measures as moving, changing their commute, taking a self-defense class, avoiding being alone, or avoiding certain locations as mentioned above in tangible costs (Anti-Defamation League, 2019; Turgoose et al., 2021); this is an instance where harms may be multifaceted and have tangible financial costs as described above *and* intangible harms, as described here. For the purpose of cost estimation, we have separated their component parts into the tangible and intangible categories. Costs of TFA can have additional intangible effects as well, such as loss of anonymity and legitimacy, that further carry over into the offline world (Anderson & Wood, 2020, 2021).

Social Costs to Society. Victims' withdrawal from participating in the community and

60

difficulty accessing sufficient support may have social costs for society as well as the victim. Victims are often blamed for any harms they suffer, especially if they do not otherwise conform to common moral expectations for sexual behavior (Marques & Rinaldi, 2020), thus contributing to the perpetuation of myths about TFA abuse. Social support for TFA survivors from friends and family and even from victim service providers and the criminal justice system may also be reduced if victims are perceived to have caused their own problems (e.g., Bailey & Mathen 2017; Benedick, 2017; Lenhart et al., 2016; Advisory Board Discussions).

Furthermore, abusers can retaliate against survivors by targeting their loved ones or wider social networks with cyber or offline violence, multiplying the harms experienced past the victim to their wider social circles (Clevenger & Navarro, 2021). Additional social consequences can include victims isolating themselves from friends or family, increased conflicts with friends or family, and loss of interest in daily activities generally (Fissel & Reyns, 2020; SME Interviews).

Beyond the direct social costs described above, TFA might harm society more generally if non-victims also take costly preventive measures to avoid victimization. For example, people who are concerned about becoming a TFA victim might avoid certain online activities that might otherwise provide them with benefits, purchase expensive equipment or software to reduce their risk of victimization, etc.

Differential Experiences of Harm by Specific Victim Groups

Some harms of TFA are experienced in particularly acute ways by certain victim groups (Bailey & Mathen 2017; Bailey & Shayan 2021; Citron & Franks, 2014; Hall & Hearn 2019). Approximately one-third of general, non-IPV specific online harassment "appears to be a result of the target's protected characteristic, such as race or ethnicity, religion, gender identity, sexual orientation, or disability. LGBTQ+ individuals, Muslims, Hispanics, and Blacks face especially high rates of identity-based discrimination" and online harassment (Anti-Defamation League, 2019; see also Lenhart et al., 2016b; Bailey & Mathen, 2017) even outside of IPV-related TFA victimization.

Non-white Victims. Few data sources exist that capture national-level statistics on TFA experiences by race/ethnicity, though a few data collections are described above in the victimization prevalence section of this report. As a reminder, while the BJS (2019) stalking report found few differences by race with the exception of American Indian/Alaska Natives and multiracial people, the Anti-Defamation League (ADL, 2022) survey found that non-white individuals were more likely than white individuals to report having suffered online hate and harassment. In a recent study conducted by Eaton and colleagues (2022), survey results revealed that individuals who experienced sexual intimate partner violence prior to the COVID-19 pandemic were at greater risk for sextortion during the pandemic. Of those who previously experienced sexual IPV, Native Alaskan and Indigenous North American women were 6.77 times more likely than white women to experience sextortion during the pandemic. The odds of sextortion during the pandemic were even greater for Black/African American women when compared to white women (OR=7.33).

The ADL's online hate and harassment survey (2022) also asks respondents to report on the harms that resulted from their experiences with online hate and harassment (ADL, 2022). Respondents were asked whether they had trouble sleeping, trouble concentrating, or felt anxious as the result of their experiences with online hate and harassment. Black/African Americans, and Asian Americans were more likely to report having experienced adverse conditions resulting from online TFA than victims of TFA in general. Approximately 20% of TFA victims in general indicated that they had trouble sleeping or concentrating or felt anxious. When considering these adverse experiences among subgroups of victims, the findings revealed racial/ethnic differences with 23% of Asian Americans, 22% of Black/African Americans, and 18% of Hispanics reporting having experienced these harms. While these estimates provide some insight into the differential experiences of harm resulting from general TFA, additional research is needed to consider whether these differences exist among the other types of harm described in this review.

Immigrant and Indigenous Victims. Immigrant and indigenous victims and survivors can each face additional loss of critical family or cultural support after TFA victimization, and immigrants particularly may suffer the threat of deportation and/or losing visa sponsorship (Henry et al., 2021). Definitions of inappropriate or harmful behavior also differ between indigenous and/or immigrant cultures; for example, circulating images of women with uncovered heads may be considered a serious transgression in some communities (Henry et al., 2021). Culturally specific stigmas that may attach to victimization can strongly impact harms suffered and access to help.

LGBTQ+ Communities. Recent estimates reveal that members of LGBTQ+ communities are more likely to report having experienced TFA in their lifetime compared to individuals who identify as heterosexual (Vogler, Kappel, & Mumford, 2023). NORC's recent 2022 survey revealed that 86% of respondents who identified as trans or non-binary have experienced TFA in their lifetime. Members of LGBTQ+ communities were more likely to report having experienced TFA compared to heterosexual individuals (81% and 68%, respectively). Similar estimates were revealed in the ADL's annual survey of online hate and harassment (2022). Specifically, 66% of LGBTQ+ respondents to the 2022 ADL survey reported having experienced some form of online harassment during the lifetime. Fifty-four percent of individuals who identified as LGBTQ+ indicated that they have experienced any severe form of online harassment in their lifetime (e.g., physical threats, sustained harassment, stalking, sexual harassment, doxing, and/or swatting).

These disparities in victimization translate to a greater risk of experiencing the associated harms/costs among members of LGBTQ+ communities, some of which may be unique to this population. LGBTQ+ survivors of TFA, especially doxing or IBSA, may be outed and/or lose family support (Waldman, 2019; Clevenger & Navarro, 2021). Waldman (2019) found that gay and bisexual men are more likely to be victims of revenge porn than the general population and the broader LGBTQ community (see also Afrouz, 2021). Furthermore, same-gender IPV, including cybermonitoring or cyberstalking, is frequently taken less seriously and people are less likely to recommend help for these victims than for opposite-sex IPV victims (Messinger et al., 2021). Results from the ADL's annual survey of online hate and harassment revealed that individuals who identified as LGBTQ+ were significantly more likely to report having experienced trouble sleeping, trouble concentrating, or feeling anxious as the result of online hate and harassment compared to other marginalized groups and in general (ADL, 2022): 38% of

LGBTQ+ respondents indicated they had experienced these harms compared to 20% of all respondents who indicated prior online harassment. Members of LGBTQ+ communities were also significantly more likely to report fear of being harassed, threatened, or otherwise targeted online in the future when compared to other respondents (45% and 22%, respectively). Recent research has also found that individuals who previously experienced sexual IPV prior to the COVID-19 pandemic and self-identified as bisexual or lesbian reported the highest rates of sextortion during the pandemic (8.9% and 7.1%, respectively; Eaton et al., 2022).

Male/Female Differences. Women and girls, women with disabilities, women in rural areas, young women, and migrant women are also disproportionately likely to be targeted by cyberviolence according to several studies (e.g., Afrouz, 2021). For example, Eaton and colleagues (2017) found that 15.8% of women surveyed had experienced threats or acts of IBSA compared to 9.3% of males, making them 1.7 times more likely to be victims of IBSA than males. However, recent research reveals that there may be a shift in the disparity between females and males in TFA victimization, with an increasing number of males reporting experiencing various forms of TFA than in previous studies. For example, Powell and Henry (2019) conducted an online survey with 2,956 Australian adults and did not find a significant difference in lifetime reports of technology-facilitated sexual violence between males and females (see also ADL, 2022). However, Powell and Henry's results did reveal some notable male-female differences in the *types* of TFA experienced. Males reported higher levels of IBSA and gender and/or sexuality-based harassment than females, whereas females reported higher levels of sexual harassment victimization. A recent survey also found that sextortion was experienced more often by males than females, since the onset of the COVID-19 pandemic, and that previous offline sexual IPV was often a mediating factor (Eaton et al., 2022).

Various cultural contexts in which gender inequality exists mean that sexuality-related harms, such as those from having a naked image of oneself distributed online without permission for example, can carry a disproportionately higher risk of subsequent sexual violence and abuse for women than for men (Henry & Powell, 2018). This greater risk makes the fear of sexual violence a key dynamic upon which abusers play when perpetrating technology-facilitated coercive control and is important to consider in understanding its impacts and costs (see Harris & Woodlock, 2019; Dragiewicz, 2021). Women may also suffer gender-based shame, fear, dread, powerlessness, and feelings of sexual violation when victimized (Marques, 2021). Female victims in one study were almost three times as likely to say that TFA "made them feel scared, and twice as likely to say the harassment made them feel worried" than male victims (Lenhart et al., 2016b; see also Flach et al., 2017). The ADL (2022) also found that women who experience TFA are more likely to report fear of future online harassment (51%) compared to males (34%).

Similarly, research has found that women victims who either endured or were targets of NCP reported lower levels of psychological well-being than women non-victims, and higher somatic symptoms than male victims of IBSA (Ruvalcaba & Eaton, 2019). The ADL (2022) reported that females who experienced online harassment were also more likely than males to report being harmed economically (11% and 7%, respectively). Additionally, females who were harassed online were more likely to report issues with sleep, concentration, or anxiety (24% female and 16% male victims) and depressive or suicidal thoughts (16% female and 10% male victims; ADL, 2022). In summary, certain victim groups are at greater risk of experiencing TFA,

which differentially exposes them to the harms/costs associated with TFA. Research also indicated that TFA-related harms/costs may impact different victim subgroups in different ways.

Although some harms/costs appear to vary by victim subgroup, research has demonstrated that the differences are generally consistent across different types of TFA; all result in long-lasting impacts on survivors. One effect of ongoing TFA is the constant vigilance that results from never being sure that the abuse is really over and that there will be no new harms to deal with (Advisory Board Discussions). Survivors of IPV-related TFA might constantly monitor their financial security, access to the job market, and other resources. They may also suffer the effects of long-term "gaslighting"—being told they are making it all up—and living in the resulting state of confusion. Feelings of technology distrust, of their abuser being omniscient and omnipresent, and of insecurity can persist for years. Financial debts, psychological issues, fear of harassment interrupting social gatherings, and other harms can be lifelong if a survivor's fundamental sense of trust is destroyed (SME Interviews; Advisory Board Discussions). Social media and Google search results can be preserved forever and re-traumatization occurs every time a survivor must share what happened. There is always fear that the abuser or the posted material will resurface again and cause new harm (Advisory Board Discussions).

Given how persistent and long lasting the harms of TFA can be, it is important to begin quantifying these harms, to get a sense of the size of the problem, and to estimate how much these harms cost victims and society. Detail about the scope and costs of these harms can be used to support the investment of resources to assist victims and prevent future crime. Since the pandemic has certainly played a role in shifting some of the distribution of experiences of harm from TFA across various groups, it will be important to ask whether the incidence of TFA, the harms suffered, and the costs incurred are greater for women and minors, transgender, gender nonconforming, and LGBTQ+ communities than to cisgender adult men, as well as how these manifest among different racial and ethnic groups.

Final Survey Instrument: Development Process and Methodology

All work discussed to this point was conducted to support the drafting, construction, and administration of the national survey which was used to estimate TFA prevalence, financial costs, and harms. The survey design tasks were co-led by Drs. Lugo-Graulich, Cohen, and Gann, and the survey was administered by IPSOS via their KnowledgePanel platform.

Sampling Methods and Survey Methodology. The KnowledgePanel, per IPSOS, is the largest online panel representative of the adult U.S. population. Formerly administered by GfK, KnowledgePanel was previously used for an NIJ-sponsored study on the public's willingness to pay to reduce white-collar and corporate crime (Simpson, Cohen, & Loughran, 2015). IPSOS's recruitment process employs an addressed-based sampling methodology from the latest Delivery Sequence File of the USPS, a database with full coverage of all delivery points in the U.S. As such, samples from KnowledgePanel cover all households regardless of their phone status, providing fully representative online samples to the research community.

Responses received via IPSOS are first weighted based on demographic characteristics and representation of known hard-to-reach populations, and then further study-specific weights are fitted via an iterative proportional fitting (raking) procedure to account for differential nonresponse or under-coverage in the actual responses received. See Appendix 3 for greater detail on the KnowledgePanel's recruitment, sampling, and weighting methodologies.

The targeted number of responses for the survey was 2,500 English and Spanish-speaking respondents from around the U.S. After consultation with IPSOS, it was determined that existing national representativeness of all age groups in the KnowledgePanel precluded the need to oversample individuals aged 18-20 who would be expected to have higher victimization rates. Adequate representation of this demographic provides confidence in estimates of prevalence for minors, as respondents recalling incidents as far back as four years will have been as young as 14 years old at the time of victimization.

Survey Development and Content. The survey contained three key components. Part 1 provides nationally representative data on the prevalence of IBSA, doxing, and cyberstalking. Part 2 focuses on the experience of victimization harms and individual tangible costs of each type of harm in a bottom-up fashion. Part 3 centers on the top-down method of estimating the public's willingness-to-pay to reduce victimization (irrespective of respondents' personal experiences), developed based on a "best-practice" protocol for a DCE survey including pre-design advice from our expert panel of advisors, online cognitive testing of the survey instrument via the Prolific platform, and pre-testing by IPSOS after the survey was built. The discrete choice experiments, in which victimization scenarios are presented to respondents who are then asked to select their preferred choice to reduce that victimization from several distinct options, were used to estimate respondents' willingness to pay to avoid or remedy these types of victimization.

Our expert Advisory Board provided insightful reactions to an early survey draft during the third meeting in January 2022. Project partners at NNEDV and CCRI provided ongoing consultative input throughout subsequent development phases; they were instrumental in helping

the project team get the abuse definitions and the prevalence and harms questions right, as well as in providing input on respondents' likely reactions to, and ability to comprehend, the DCE questions. Their input was crucial in helping tailor the survey to be victim sensitive and the questions to be clear to the average respondent ahead of the cognitive testing process.

Part 1 of the survey asked respondents if they have experienced any of the victimization types being studied. Those that answered "yes" to any of the scenarios presented then answered several questions about the victimization experience(s) they disclosed. They only answered the follow up questions associated with the particular victimization they disclosed. Those respondents were asked whether their victimization (or the most recent incident if they experienced this victimization at the hands of multiple people) occurred during the last 12 months, more than 12 months ago but after the COVID-19 pandemic began (March 2020), or before 2020. To avoid telescoping memory problems, the decision was made to use the pandemic as a benchmark event. Analyses also looked at changes in incidence before, during, and after the height of the pandemic. Note that the purpose of these questions was to estimate prevalence in the population, not to create annual estimates. Moreover, these types of crimes are often perpetrated over several months or even years, making lifetime prevalence the relevant question for these purposes with a couple of benchmarks for anchoring. Other questions asked whether their perpetrator was a current or former intimate partner, whether they were subsequently able to get their information removed from the internet, and other contextual questions.

If the respondent disclosed victimization from IBSA, doxing, and/or cyberstalking, they were directed to Part 2 of the survey which asked what harms they suffered, what tangible costs they incurred as a result of the victimization, and about how much those different expenses cost them. Those who did not disclose any victimization skipped ahead to Section 3 and the DCEs. For those answering questions in the harms section, the possible harms they could select were grouped in the same categories as in the taxonomy presented above. Due to the anticipated difficulty that some polyvictims would have reporting on which harms occurred as a result of which victimization type, and to reduce reporting burden on the part of the respondent, these questions were asked once for all victimizations. Differences in harms experienced based on single or multiple victimizations, or by particular victim groups, are be parsed out in the analysis discussed below.

All respondents, whether or not they experienced TFA victimization personally, answered the DCE questions where they were asked their willingness to pay for varying levels of TFA reduction (including a zero-dollar, "do nothing" option as described earlier in the literature review). One interesting challenge in constructing this survey, compared to previous online surveys using these methodologies, was adjusting for the fact that most respondents to online surveys now complete them on their mobile phones rather than on a laptop or desktop computer. This shift meant that many parts of the survey had to be redesigned from initial conceptions based on earlier research, such as the example from Box 1 above. For example, matrix questions in which respondents can tick a series of radio buttons on several items in a row no longer work; they do not display well on a phone screen. Text-heavy definitions had to be shortened and multi-part questions separated into individual questions, not all of which could appear on the same screen at the same time. The authors worked closely with IPSOS to painstakingly redesign the survey given this new dominant format while still retaining the original intent and purpose of

each question and section. One result was that the DCEs were split up to ask first about cost preferences for different levels of reduction, then separately about policy preferences for whether public or private funds should pay for reductions, and then another separate question about the types of programs they would support (victim assistance, stronger punishment, and/or technology protections). In previous DCE studies, these were all combined into the DCE "bundles" from which a respondent could choose.

Lastly, although the KnowledgePanel data automatically include a wide range of demographic characteristics collected prior to our survey, additional questions were also included to control for political differences such as opinions about the role of government spending and other factors that might influence the DCE responses. With these questions about tangible costs (bottom-up method), the DCE results (top-down method), and the prevalence estimates we generated from our sample of 2,521 respondents, we are able to provide improved insights into the costs of TFA to victims and to the U.S. The final survey instrument can be found in Appendix 1.

Cognitive Testing Process. Prior to programming the survey with IPSOS, two waves of cognitive testing of the instrument were conducted via the online Prolific platform, which is similar to Amazon's mTurk but offers more flexible capabilities such as the ability to test certain questions only with those who had been victims of harassment, for example. The cognitive testing invited individuals to answer the draft survey questions and then answer open-ended questions about the comprehensibility and clarity of the questions, including whether the order in which they were presented made sense. Respondents only received payment if they completed the entire survey. Tests were conducted separately of the prevalence and harms section and the DCE section; while most respondents expressed little difficulty in understanding the questions in the much later drafts tested, others provided valuable input and adjustments based on that input were made to the instrument.

IPSOS Pre-testing and Survey Administration. Both the pre-test and final surveys were fielded in English and Spanish. Once the cognitive tests were completed and questionnaire revisions made, the project team began working with IPSOS to prepare the survey for programming. This included revising the survey to function well in a mobile environment. Additionally, IPSOS's survey methodologists offered additional expertise in optimizing various questions to generate the most valid responses and to encourage respondents to complete the entire survey. Once IPSOS finished programming the survey, two rounds of pre-testing in its KnowledgePanel system with 25 KnowledgePanel members were conducted to assess: (1) average length of time required to complete the survey, (2) remaining difficulty in understanding the survey questions, and (3) internal respondent consistency. These pre-tests were conducted in early November 2022.

The final survey was fielded from November 10-21, 2022. A random sample of 4,167 panel members was drawn from IPSOS' KnowledgePanel. 2,521 (excluding breakoffs) responded to the invitation and 2,521 qualified for the survey, yielding a final stage completion rate of 60.5% and a qualification rate of 100%. After the survey was completed, IPSOS calculated the survey weights and provided the raw data file with weights, standard demographic information, and some additionally purchased demographics for all respondents to JIRN for

analysis. The final, complete survey instrument can be found in Appendix 1, and the detailed survey methodology can be found in Appendix 3.

Analytical Plan

Once the final survey dataset with weights was received from IPSOS, JIRN staff conducted the following analysis activities. First, JIRN staff cleaned the data for typographical errors and needed variable transformation. Next, we generated descriptive analyses of the demographics of the survey sample compared against U.S. census population distributions, along with crosstabulations that described the victimization patterns and rates observed, reported costs incurred by victims, the general willingness of the sample to pay to avoid or remedy TFA victimization, as well as their answers to the control questions about factors that may also influence respondents' DCE choices.

From there, we estimated prevalence rates of cyberstalking, IBSA, and doxing, both generally and with a current or former intimate partner as perpetrator. These were estimated for the U.S. as a whole and broken down by various subpopulations as much as possible. The unit of analysis was individuals (as opposed to occurrences of one of the types of TFA). Care was taken in choosing the unit of analysis for counting, since IPV, cyberstalking, and harassment are ongoing patterns of repeat victimization rather than single, discrete events (Lauritsen & Rezey, 2013). Furthermore, posting images on the internet may be a one-time act, but it has been argued that that each new viewing or sharing of such an image constitutes a revictimization (*Paroline v. United States*, 2014). However, because our interest in this study is estimating a nationally representative estimate of TFA prevalence, we decided to use individuals as the unit of analysis.

Brown and colleagues (2021) also noted the importance of considering multi-dimensional patterns of victimization and their impacts on victims. Davis et al. (2019) suggested that researchers should consider the various characteristics of victimization experiences that may be associated with increased risks for negative outcomes (i.e., polyvictimization, known perpetrator, negative social reactions, and perceived threats to life or safety). Finally, these victimizations are also not uniform in distribution in that a small portion of the population may be victimized heavily and repeatedly. Consideration was given to the costs of these victimizations borne by those other than the direct victim, such as family, spouses, the victim's employer, and others based on survey responses and the cost burdens identified in the taxonomy of harms. The survey was constructed to analyze several of these types of questions by using the questions our team designed, the canned demographics provided by IPSOS for all KnowledgePanel respondents, and the purchase of some additional questions that IPSOS has also previously asked all respondents.

After prevalence estimation analyses were completed, the discrete choice experiment (DCE) responses were analyzed to generate holistic victimization cost estimates. This task involved statistical modeling and empirical estimation. We modeled the willingness-to-pay to reduce crime as WTP = f(x1, x2, x 3, x 4…..x.n), where WTP is a function of underlying factors. Among the factors we isolated through the survey design were the type of crime, preferences for different programs designed to mitigate its prevalence or consequences, victimization status, and demographic characteristics of the respondent. Multiple regression analysis was used to estimate the effects of these factors on the public's willingness-to-pay.

The DCE analyses include many different comparisons and attempts to understand the underlying preferences of citizens on TFA harm mitigation. Several of the hypotheses listed here also involve sub-hypotheses generated prior to beginning the actual analyses based on the background work conducted to date and presented in this report. The following list is a general overview of the analyses that were conducted.

1. *Estimate the monetary value of TFA crimes.* The survey provided nationally representative estimates of the "willingness to pay" to reduce three TFA offenses, both generally and within IPV, which may be converted into the "cost of crime."

2. *Comparison of "out-of-pocket" costs of crime to public's willingness-to-pay for TFA crime reduction.* The public's total valuation of crime reduction exceeds the out-of-pocket costs of crime for crimes that have been previously studied using willingness-to-pay. We test this in relation to TFA. This has important policy implications for regulatory analysis (including cost-benefit analysis) and enforcement priorities.

   H_1: Measured financial losses incurred are lower than public WTP to avoid such losses.

3. *Characterize the degree of variability in public preferences and willingness-to-pay.* By collecting demographic information, we were able to begin to characterize the extent to which public preferences and willingness-to-pay vary by individual. For example, Cohen et al. (2004) demonstrated an increased WTP with income and victimization risk factors such as race, ethnicity and age, and the L-RAT theoretical perspective also suggests that there may be some variation here.

   H_2: There is significant variability in reported WTP based on group victimization risk; members of higher-risk groups are more likely to value TFA crimes higher than lower-risk groups.

   H_3: There is significant variability in reported WTP based on prior victimization experience; victims of TFA are more likely to value TFA crimes higher than nonvictims.

4. *Comparison of the public's valuation of alternative policy instruments for reducing TFA victimization.* Using the questions on policy preferences and preferences for public or private payment, we were able to examine whether the public views increased criminal punishment more desirable, for example, than increased victim mitigation. These hypotheses are informed by the bounded rational choice and social learning frameworks:

   H_4: Reported WTP will be higher for identical scenarios when respondent prefers programs to mitigate victim harm rather than policies that increase punishment.

   H_5: Reported WTP will be higher for identical scenarios when respondent prefers government to pay for programs to reduce victimization rather than technology companies that pass costs onto consumers.

5. *Feasibility of determining prevalence of TFA victimization.* The prevalence estimation analyses have the potential benefit of testing the feasibility of using a nationally representative survey to determine the prevalence of TFA victimization, as well as serving as the multiplier base for national estimates of the costs associated with these crimes. Hypotheses are informed by L-RAT and conservation of resources (COR) theories.

   H_6: Prevalence rates will vary by victim characteristics such as demographics, polyvictimization, and perceived threats to safety in online activity.
   H_7: Polyvictimization rates will vary by vulnerability characteristics, such as knowing the perpetrator and previous TFA victimization.

6. *Estimating average tangible costs experienced by victims of TFA.* By asking respondents who self-disclosed experiencing victimization to share the types of costs they incurred and how much their losses were, we were able to estimate some ranges of out-of-pocket costs caused by TFA in the short and long term. Average costs were disaggregated by victim groups to assess average differences in harms experienced.

Finally, the project's prevalence rates and DCE cost estimates were compared against currently available information in the existing data sources described in the literature review to assess their comparability. We estimated lifetime and past-year prevalence. In the literature review, TFA rates appeared to be higher than more traditional (in-person) forms of victimization on average, perhaps due to the convenience and ease of technology. Below we discuss how this has held true when comparing our survey results to recent, comparable in-person victimization rates.

Data

This section discusses the operationalization of the survey measures used in the analyses. In addition, we present the descriptive statistics for all relevant independent and dependent variables (i.e., victimization prevalence rates).

Dependent Variables

The primary dependent variables in this study are five dichotomous measures of TFA victimization: IBSA, cyberstalking, doxing, any TFA victimization, and polyvictimization (i.e., experiencing two or more types of TFA victimization). Each outcome variable was coded as *0=No, 1=Yes*. The descriptive statistics for each of the five outcome measures are presented in Table 6. The 'Lifetime Prevalence' figures indicate whether respondents experienced TFA at any point in their life, while the '1-Year Incidence' figures indicate whether respondents experienced TFA within the 12 months prior to completing the survey.

Table 6. Descriptive Statistics for Victimization Experience (Weighted)

Measure	Lifetime Prevalence			1-Year Incidence		
	# Experiencing TFA	Percent	95% CI	# Experiencing TFA	Percent	95% CI
IBSA	193	7.7	6.6 - 8.9	26	1.1	0.5 - 1.5
Cyberstalking	187	7.4	6.4 - 8.6	45	1.8	1.3 - 2.4
Doxing	137	5.4	4.5 - 6.5	44	1.8	1.3 - 2.4
Any Victimization	403	16.0	14.5 - 17.6	99	3.9	3.2 - 4.8
Polyvictimization	94	3.7	3.0 - 4.7	41	1.6	1.1 - 2.3

Image Based Sexual Abuse (IBSA)

This variable indicates whether respondents experienced IBSA. Specifically, respondents were provided with the definition of IBSA and asked two questions:

> Sometimes people threaten to share or actually share images or videos of others that are partially nude, nude, or sexually explicit without the consent of people in the images. These images could be real, faked, or altered. This is called **image-based sexual abuse**.

> Regardless of whether or not the images or videos were actually shared, has anyone ever **threatened** to share real or fake partially nude, nude, or sexually explicit images or videos of you without your consent?

> Regardless of whether or not you were threatened, has anyone ever **actually shared or posted** any real or fake partially nude, nude, or sexually explicit images or videos of you without your consent?

IBSA was the most common single type of lifetime TFA victimization in the sample (7.7%), but it was the least common single type that occurred in the past year (1.1%)

Cyberstalking

This variable indicates whether respondents had ever been a cyberstalking victim. Because cyberstalking can involve many different actions, respondents were asked to provide yes/no answers to seven possible types of cyberstalking:

> Sometimes people use technology to repeatedly harass another person, spy on them, or monitor or interfere with their activity. This is called **cyberstalking**. Has anyone ever done this to you?
>
> 1. I received unwanted and repeated texts, emails, or social media messages (does not include spam or phishing emails or texts)
> 2. Someone monitored my social media, email, financial, or other accounts and communications to track my activities
> 3. Someone installed stalkerware or spyware on my phone or computer (such as a key logger)
> 4. Someone changed my login information or security settings on my devices or social media accounts
> 5. Someone impersonated me to interfere with my personal or work relationships, cancel important events (like court dates), or run up debts
> 6. Someone tracked my location using technology (such as a GPS tracker, mobile phone, digital doorbell)
> 7. Someone watched me using devices that I did not know about

The lifetime prevalence of cyberstalking in this study (7.4%) was slightly less than that for IBSA, but slightly higher (1.8%) than IBSA when focusing on past year victimization experiences.

Doxing

This variable indicates whether respondents had experienced doxing. Similar to the previous two TFA measures, respondents were first given a brief definition of doxing and then asked whether they had ever been victimized:

> **Doxing** is when someone releases your personal contact or sensitive information (other than photos or videos) to others without your consent. <u>Note</u>: this does not include mass data breaches, which occur when hackers steal your private information from a credit card company or other data sources.

> Has anyone ever doxed you by publicly posting your work/school/home address, phone number, social security number, social media accounts, sexual history, or medical or financial information online without your consent?

Doxing lifetime prevalence (5.4%) among the three individual TFA measures used in this study, but the 1-year incidence rate was equal to that of cyberstalking (1.8%).

Other TFA Victimization Variables

Finally, we created two composite victimization variables: *Any Victimization* and *Polyvictimization*. The *Any Victimization* measure indicates whether respondents experienced any of the three TFA victimization types included in this study. As expected, this measure had the highest lifetime prevalence (16.0%) and 1-year incidence (3.9) rates. Conversely, the *Polyvictimization* measure—which indicated whether respondents had experienced two or more types of TFA—had the lowest lifetime prevalence at 3.7%, though the 1-year incidence rate for polyvictimization (1.6%) was slightly higher than that of IBSA.

Independent/Control Variables

A number of independent variables were included in the study to provide context for the TFA victimization prevalence rates and DCEs. The tables below provide both weighted and unweighted descriptive statistics for the demographic, ideological, internet safety, and mental health variables included in this study. Most of these demographic variables were already provided by IPSOS as background information for their sample. For the demographic variables (see Table 7), we also included descriptions of the general U.S. population as these figures were used in the weighting process. The general population estimates were obtained from the U.S. Census Bureau's Current Population Survey (CPS) and American Community Survey (ACS; see Appendix 3 for more detail on the weighting process).

Demographic Variables

Only one demographic variable from our survey sample—median age—was significantly different compared to the corresponding general population estimate. The median age among the survey respondents was 47 years old, whereas according to the 2022 Current Population Survey the median U.S. age was approximately 40 years old.

The weighted demographics for the remaining measures were quite similar to the general population estimates taken from the CPS and ACS. Sixty-two percent of the sample were White, 12% Black, 1.4% multiracial, and roughly 7% identified as another race. Seventeen percent of survey respondents were Hispanic. Approximately 47% of survey respondents self-identified as male, while 49% identified as female. The remaining respondents identified as transgender (0.5%), non-binary (0.6%), or something else (0.4%). Regarding respondents' sexual orientation, 91% of the sample indicated they were straight, 3.4% bisexual, 2.9% gay/lesbian, and 2% other.

As shown in Table 7, these distributions closely mirror those found in the general population. Over half of the respondents (55.6%) were married at the time of the survey, while another 30% had never been married.

The regional breakdown of respondents was nearly identical to the general population estimates: 17.4% resided in the Northeast, 20.6% in the Midwest, 23.7% in the West, and 38.3% in the South. Approximately 35% of the weighted sample had a college degree, while 29% had only a high school diploma or GED and 10% did not graduate high school. Almost half of the sample (49%) were working full-time. Another 14% were working part-time, and 36% were not working. Finally, there was significant distribution among respondents' household income. About 29% made less than $50,000 per year, while 43% made more than $100,000 per year.

Table 7. Sample Descriptives for Primary Demographic Variables

	Unweighted Sample (%)	Weighted Sample (%)	General Population (%)
Age	Mean: 50.5 Median: 52.0	Mean: 48.0 Median: 47.0	Median: 39.8
Gender Identity			
Male	48.8	46.5	47.2
Female	47.0	49.2	50.5
Transgender	0.4	0.5	0.6
Non-Binary	0.6	0.6	-----
Other	0.4	0.4	1.7
Sexual Orientation			
Gay/Lesbian	2.9	2.9	3.3
Straight	91.2	90.5	88.3
Bisexual	3.0	3.4	4.4
Other	1.7	2.0	1.9
Marital Status			
Married	58.5	55.6	48.0
Widowed	4.2	3.7	5.5
Divorced	9.5	8.7	10.6
Separated	2.0	2.2	1.7
Never Married	25.9	29.9	34.2
Race/Ethnicity			
White	68.2	62.0	58.1
Black	9.9	12.0	11.8
Hispanic	13.1	17.2	18.8
Other	5.2	7.3	7.0
2+ Races	3.6	1.4	4.3
Education			
No HS Diploma	7.2	9.6	10.8
HS/GED Diploma	28.2	29.2	27.3
Associate's or Some College	25.8	26.4	29.5

Bachelor's Degree	21.1	19.0	20.3
Graduate Degree	17.7	15.8	12.2
Region			
Northeast	17.9	17.4	17.1
Midwest	21.8	20.6	20.6
South	37.2	38.3	38.6
West	23.2	23.7	23.6
Household Income			
< $10,000	3.1	3.9	6.0
$10,000-$24,999	7.0	8.6	11.4
$25,000-$49,999	17.0	16.1	19.1
$50,000-$74,999	15.8	15.8	16.8
$75,000-$99,999	13.7	12.7	12.8
$100,000-$149,999	16.7	18.3	16.3
> $150,000	26.7	24.6	17.7
Employment Status			
Full-Time	49.0	48.9	-----
Part-Time	13.8	14.2	-----
Not Working	37.2	35.9	-----

Political Measures

Survey respondents were asked to answer three questions regarding their views on political issues.

1. In general, how do you see yourself?
2. How do you see yourself on social issues?
3. How do you see yourself on economic issues?

These questions used a 7-point Likert scale, ranging from (1) Very Liberal to (7) Very Conservative. As shown in Table 8, when asked about their general political leanings, 29% stated they were liberal, 35% moderate, and 35% conservative. A similar distribution was found when respondents were asked their political views on social issues: 32% liberal, 33% moderate, and 34% conservative. Political views on economic issues, however, leaned more conservative; over 40% identified as economically conservative, with 33% moderate and only 23% liberal.

In addition, respondents were asked "In general, do you believe taxes are too high, about right, or too low?" Less than 6% responded that taxes were too low; 64% stated taxes were too high, and the remaining 30% said they were about right. Unsurprisingly, there was a very strong correlation (p<.01) between respondents' views on taxes and their political leaning on economic issues: those who identified as economically conservative were significantly more likely also to state that taxes were too high.

Table 8. Sample Descriptives for Political Measures

	Unweighted Sample (%)	Weighted Sample (%)
General Political Leaning	Mean: 4.14 Median: 4.00	Mean: 4.11 Median: 4.00
Very Liberal (1)	5.4	5.4
Liberal (2)	14.9	14.9
Slightly Liberal (3)	8.3	8.3
Moderate (4)	34.1	35.4
Slightly Conservative (5)	10.9	10.5
Conservative (6)	18.1	17.2
Very Conservative (7)	6.9	6.8
Social Issues	Mean: 4.04 Median: 4.00	Mean: 4.03 Median: 4.00
Very Liberal (1)	7.1	6.8
Liberal (2)	15.2	15.0
Slightly Liberal (3)	10.0	9.9
Moderate (4)	31.9	33.4
Slightly Conservative (5)	10.6	10.4
Conservative (6)	16.9	16.1
Very Conservative (7)	7.0	7.0
Economic Issues	Mean: 4.47 Median: 4.00	Mean: 4.43 Median: 4.00
Very Liberal (1)	3.9	4.0
Liberal (2)	10.5	10.4
Slightly Liberal (3)	8.2	8.5
Moderate (4)	31.4	33.2
Slightly Conservative (5)	12.5	12.0
Conservative (6)	21.4	20.3
Very Conservative (7)	10.7	10.2
Taxes	Mean: 2.58 Median: 3.00	Mean: 2.59 Median: 3.00
Too Low (1)	6.0	5.8
About Right (2)	29.5	28.8
Too High (3)	63.3	64.2

Internet Safety Measures

Respondents were asked two questions regarding their use of social media and their level concern about sharing personal information online. As shown in Table 9, 58% of the weighted sample indicated that they regularly check and/or post on social media. In addition, when asked how concerned they are about providing personal information over the internet, 6% said they were not concerned at all, 25% were slightly concerned, and 68% were either somewhat or very concerned.

Table 9. Sample Descriptives for Internet Safety Measures

	Unweighted Sample %	Weighted Sample %
Do you regularly check/post on social media?		
Yes	56.0	58.3
No	42.6	40.2
How concerned are you about providing personal information over the internet?	Mean: 2.97 Median: 3.00	Mean: 2.95 Median: 3.00
Not at all concerned (1)	5.4	6.1
Slightly concerned (2)	25.1	25.3
Somewhat concerned (3)	36.2	35.7
Very concerned (4)	32.9	32.5

Mental Health Measures

Finally, all respondents were asked to indicate whether they had been diagnosed by a medical professional with any of four mental health conditions: anxiety disorder, depression, mood disorder, or post-traumatic stress disorder (PTSD). We also created a composite mental health variable that identifies whether respondents had been diagnosed with any of the four conditions. As shown in Table 10, the most common individual type of reported mental health condition was depression (16.1%), followed closely by anxiety disorder (16%). Mood disorder (2.3%) and PTSD (5.5%) diagnoses were significantly less common among the survey respondents. When combined, roughly one-quarter of respondents had been diagnosed with at least one of the four mental health conditions.

Table 10. Sample Descriptives for Mental Health Measures

	Unweighted Sample (%)	Weighted Sample (%)
Diagnosed with anxiety disorder		
Yes	15.4	16.0
No	84.6	84.0
Diagnosed with depression		
Yes	15.9	16.1
No	84.1	83.9
Diagnosed with mood disorder		
Yes	2.1	2.3
No	98.0	97.7
Diagnosed with PTSD		
Yes	5.3	5.5
No	94.7	94.5
Diagnosed with any of these		
Yes	23.1	23.4
No	76.9	76.6

Results

This section presents the results from the analyses used to address the research questions and hypotheses discussed above. First, we present the demographic profiles of those who experienced TFA victimization. Next, we discuss prevalence rates by region of the country, whether the victim was a juvenile, and victim-offender relationship. After the binary descriptive results are presented, we discuss the reported harms and consequences suffered by TFA victims, including both tangible and intangible costs of victimization. Finally, we present the findings from the discrete choice experiment (DCE) section of the survey, including respondents' willingness to pay to reduce TFA and how to pay for TFA reduction programs. Unless otherwise noted, all descriptive and inferential statistics below are conducted using the weighted sample (N=2,521) to best generate general population estimates.

Prevalence and Incidence of TFA

As shown in Table 11, 403 out of the 2,521 respondents (16%) indicated that they had experienced at least one type of TFA in their lifetime. The most common individual offense was IBSA (7.7%), followed by cyberstalking (7.4%) and doxing (5.4%). Slightly less than 4% of the sample were victims of at least two types of TFA in their lifetime. The 1-year incidence rates present a slightly different picture of TFA victimization. Approximately 4% of the respondents had experienced at least one type of TFA in the past year. Cyberstalking and doxing were tied for the highest individual 1-year incidence rate (1.8%), with IBSA victimization being the lowest individual measure (1.1%). Finally, 1.6% of survey respondents indicated that they experienced at least two types of TFA in the past year.

Table 11. Descriptive Statistics for Victimization Experience

	Lifetime Prevalence			1-Year Incidence		
Measure	# Experiencing TFA	Percent	95% CI	# Experiencing TFA	Percent	95% CI
IBSA	193	7.7	6.6 - 8.9	26	1.1	0.5 - 1.5
Cyberstalking	187	7.4	6.4 - 8.6	45	1.8	1.3 - 2.4
Doxing	137	5.4	4.5 - 6.5	44	1.8	1.3 - 2.4
Any Victimization	403	16.0	14.5 - 17.6	99	3.9	3.2 - 4.8
Polyvictimization	94	3.7	3.0 - 4.7	41	1.6	1.1 - 2.3

*Note: Categories are not mutually exclusive. For example, someone who was a victim of both IBSA and doxing appears in four rows: IBSA, Doxing, Any Victimization, and Polyvictimization.

For each type of TFA included in the survey, respondents were asked a number of follow-up questions if they indicated they were victimized. One of the follow-up questions asked when the victimization occurred. Possible responses were:

1. In the past 12 months
2. More than 12 months ago, but after Covid-19 started (since March 2020)
3. Pre-Covid-19 (before March 2020)

As the survey was fielded in November 2022, the first response option indicates the victimization occurred in November 2021 or later, and the second response between March 2020 and October 2022. Response options for our occurrence measure were operationalized in this manner so we could examine whether there were any significant effects of the Covid-19 pandemic on TFA victimization.

As shown in Table 12, most cases of IBSA (70%) occurred prior to the Covid-19 pandemic (March 2020), and only 16% of victimizations occurred in the preceding 12 months. Conversely, 33% of reported doxing victimizations occurred during the past year, compared to 44% occurring prior to Covid-19. The figures for cyberstalking were between those for IBSA and doxing: 24% of cyberstalking victimizations occurred within the 12 months preceding the survey, and 57% occurred prior to March 2020. For those that experienced two or more types of TFA, the most recent instance occurred prior to Covid-19 for 64%, while only 19% experienced both TFA incidents within the past 12 months.

Table 12. Time Distribution of TFA Prevalence and Incidence

	IBSA	Cyberstalking	Doxing	Any Victimization	Polyvictimization
When did this occur?					
In the past 12 months	16.3	24.06	33.0	22.1	18.5
More than 12 months, but after Covid-19 started (March 2020-October 2021)	13.4	18.9	22.7	17.5	17.7
Pre-Covid-19 (before March 2020)	70.4	57.1	44.3	60.4	63.8
Total	100%	100%	100%	100%	100%

There is reason to believe that TFA would increase during the pandemic; with the switch to remote work and school, people are using the internet—and technology in general—more today than ever. For example, the National Network to End Domestic Violence (NNEDV; 2021) conducted a needs assessment of over 1,000 victim service providers in December 2021-January 2022. They found that many common types of technology abuse—harassment, limiting access to technology, and surveillance—increased significantly during the Covid-19 pandemic. In the current study we cannot directly compare rates over time since the three time periods are of varying lengths. However, in all four crime categories, the most recent 12-month time period (November 2021 to November 2022) showed higher rates than the previous 20-month timeframe (March 2020 to October 2021). Thus, it appears these crimes have increased over time, though the majority of IBSA, cyberstalking, any victimization, and polyvictimization occurred prior to the beginning of Covid-19 (March 2020).

Respondents were also asked to indicate their relationship with the person responsible for their victimization (see Table 13). Just over 40% of IBSA victims and just under 40% of cyberstalking victims indicated that the perpetrator was a current or former intimate partner, though cyberstalking perpetrators were more likely to be former intimate partners (26.6%) compared to current intimate partners (12.7%). For doxing, the modal categories were stranger

(19.9%) and unknown (30%). All of these figures are consistent with the extant literature discussed above.

Table 13. Victim-Offender Relationship at Time of Victimization

	IBSA	Cyberstalking	Doxing
Victim-Offender Relationship			
Intimate Partner	21.5	12.7	4.4
Former Intimate Partner	18.9	26.6	12.1
Family Member	0.5	3.5	1.2
Friend	4.3	5.9	6.0
Coworker	-----	3.2	2.9
Acquaintance	9.6	9.7	11.9
Stranger	18.6	17.5	19.9
Other	6.7	7.5	12.1
Unknown	20.0	13.3	30.0
Total	100%	100%	100%
Where They Met			
Online	39.5	24.6	24.2
School/College	32.8	23.6	15.1
Work	6.4	16.2	12.11
In My Neighborhood	9.7	12.2	31.2
Other	11.7	23.4	17.4
Total	100%	100%	100%

Demographic Profiles of TFA Victims

The following tables display the breakdown of those who experienced IBSA, cyberstalking, doxing, any victimization, and polyvictimization according to the demographic, ideological, internet safety, and mental health variables discussed above.[6]

Table 14 shows the 1-year incident rates of TFA victimization, or the percentage of respondents who indicated they were victims of TFA within the past year. Lifetime prevalence rates are displayed in Table 16 below. As shown in Table 14, there were modest differences in the mean ages across the five TFA measures. Doxing had the oldest average age (46.7 years) of the individual TFA types, followed by cyberstalking (45.8 years) and IBSA (39.0 years). Those who experienced polyvictimization in the past year had the youngest average age (38.6 years). In general, as respondents' age increased, their likelihood of TFA victimization decreased.

---

[6] The tables should be read from left to right. For example, the 1.27 in the Male/Cyberstalking cell in Table 14 indicates that 1.27% of those who identify as male in the sample had experienced cyberstalking in the past 12 months.

Although the minimum age of survey respondents was 18, some of the younger respondents were likely victimized when they were minors. For purposes of this report, we have estimated the number of minors by assuming the following were victimized when they were minors:

(1) All 18-year-old victims at the time of the survey
(2) All 19- and 20-year-old victims who indicated they became aware of their victimization more than 12 months prior to the survey (i.e. before November 2021), and
(3) All 21-year-old victims who indicated they became aware of their victimization prior to March 2020.

The result was that out of the 403 (weighted) victims, 53 (13.1%) were identified as likely to have been victimized when they were minors. As discussed in more detail below, this small sample makes comparisons difficult—especially once breaking the sample down by crime type. 42 respondents were victims of IBSA as a minor, 17 were victims of cyberstalking, 17 were victims of doxing, and 18 were victims of more than one type of TFA.

Note that the estimated percent of victims who were minors is likely very conservative. First, the survey asks for the most recent incident, so that we do not capture adult victims who previously victimized as minors. Second, we have not counted individuals who were age 22 or older but indicated their most recent victimization took prior to March 2020 – as we do not know if they were minors at the time.

Table 14. Victimization Experience by Demographic Variables – Past 12 Months

	Percent Experiencing TFA in the Past 12 Months				
	IBSA	**Cyberstalking**	**Doxing**	**Any Victimization**	**Poly-Victimization**
Age					
Mean	39.0	45.8	46.7	45.1	38.6
Gender Identity (%)					
Male	0.76	1.27	0.88	2.45	0.71
Female	1.24	1.97	2.39	4.94	2.04
Other[1]	4.87	4.76	4.88	9.63	6.25
Sexual Orientation (%)					
Gay/Lesbian	0.00	5.67	1.77	5.67	3.95
Straight	1.06	1.62	1.67	3.78	1.48
Bisexual	0.46	2.29	3.41	5.61	0.55
Other	3.60	2.34	3.60	5.94	5.94
Marital Status (%)					
Married	0.85	1.54	1.54	3.35	1.27
Widowed	0.00	2.49	3.74	4.65	1.58
Divorced	0.34	2.55	1.98	4.87	1.02
Separated	2.46	4.29	4.94	9.23	4.94
Never Married	1.64	1.71	1.59	4.21	2.18
Race/Ethnicity (%)					
White	0.68	1.54	0.91	2.92	1.00

Black	1.23	2.49	2.84	5.85	1.59
Hispanic	1.56	2.03	4.11	5.71	2.70
Other	2.47	1.37	1.57	4.45	3.78
2+ Races	1.85	4.84	1.35	6.69	4.07
Education (%)					
No HS Diploma	2.87	0.83	3.55	5.74	3.64
HS/GED Diploma	0.83	2.54	1.23	4.31	0.92
Some College	0.86	2.04	2.34	4.37	2.17
Bachelor's Degree	0.35	1.40	1.05	2.59	1.18
Graduate Degree	1.47	0.93	1.46	2.92	1.26
Region (%)					
Northeast	0.40	0.95	1.41	2.47	0.30
Midwest	1.22	1.55	1.87	3.93	1.97
South	1.45	2.65	1.44	4.72	2.22
West	0.70	1.16	2.39	3.66	1.29
Household Income (%)					
< $10,000	2.77	4.48	5.16	11.02	4.93
$10,000-$24,999	0.00	3.52	2.20	4.65	1.83
$25,000-$49,999	0.40	2.39	3.14	5.41	1.61
$50,000-$74,999	0.78	2.20	1.71	3.98	2.11
$75,000-$99,999	2.30	1.56	1.69	4.34	2.16
$100,000-$149,999	0.69	1.35	1.20	3.25	1.13
> $150,000	1.35	0.49	0.61	1.80	0.77
Employment Status (%)					
Full-Time	1.05	1.46	1.26	3.18	1.79
Part-Time	0.73	2.45	1.81	4.58	1.75
Not Working	1.16	1.94	2.40	4.68	1.31

[1] Includes those identifying as transgender (n=13), nonbinary (n=15), or "other" (n=10). Due to small individual sample sizes, these categories were collapsed into a single category.

Across four of the five TFA measures, White respondents were the least likely to be victimized in the past year, ranging from 0.68% for IBSA to 2.92% for any victimization. Cyberstalking was the only type of TFA in which White respondents (1.54%) did not have the lowest rates; Hispanics had a slightly lower rate at 1.37%. Conversely, multiracial respondents had the highest rates of victimization for cyberstalking (4.84%), any victimization (6.69%), and polyvictimization (4.07%). Respondents in the "other" race category had the highest rate (2.47%) for IBSA, while Hispanics had the highest rate of victimization for doxing (4.11).

For each of the five TFA measures, those who identified as non-cisgender (i.e., transgender, nonbinary, and 'other') experienced significantly higher rates of victimization in the past year compared to both cisgender males and females. These findings are comparable to the NORC (2022) study discussed above. We found similar results for respondents' sexual orientation. Straight respondents were less likely to be victims of cyberstalking, doxing, and any victimization relative to those who identify as gay/lesbian, bisexual, or another orientation. Gay/lesbian respondents (0.00%) had the lowest incidence rates for IBSA, and bisexual

respondents (0.55%) had the lowest rate for polyvictimization. Conversely, respondents who identified as gay/lesbian or another orientation had the highest victimization rates for each of the five TFA measures; in no measure did straight respondents have the highest rate.

The only discernable pattern regarding victimization rates by marital status was that separated respondents were most likely to experience each of the TFA measures compared to those who were married, widowed, divorced, or never married. This finding was somewhat expected for IBSA and cyberstalking since current or former intimate partners were two of the most common victim-offender relationships found in the data. Conversely, married respondents had the lowest rates of victimization in the past year for cyberstalking, doxing, and any victimization, while widowed respondents were least likely to experience IBSA. It is important to note, however, that these are simple correlations; we cannot infer any causality here because we do not know respondents' marital status prior to victimization.

For education level, region of residence, and employment status, there were few TFA victimization patterns found in the data. Regarding education level, those without a high school diploma had the highest 1-year rates of victimization for IBSA (2.87%), doxing (3.55%), any victimization (5.74%), and polyvictimization (3.64%), and those with a high school diploma or GED (2.54%) were most likely to experience cyberstalking. However, the differences in prevalence rates for each TFA measure were very small among the five education groups. For region of residence, there were no significant differences in any TFA victimization prevalence rates by where respondents lived. Similarly, there were no significant differences in victimization experience by respondents' employment status.

The final demographic variable we included in the analyses was household income. In general, respondents from lower income households were more likely to experience each TFA measure compared to those from higher income households, though the relationship between income and victimization was not perfectly linear. For example, those in the highest income group (> $150,000) were more likely to experience IBSA in the past year relative to four of the six lower income groups.

Table 15 presents the lifetime prevalence rates of TFA victimization (i.e., the percentage of respondents who indicated they were victims of TFA at some point in their life) by the demographic variables included in this study. As seen in the table, most of the patterns in the lifetime victimization figures mirror those from the 1-year incidence rates shown in Table 14, with the anticipated exception that the lifetime victimization rates are much larger than the 1-year rates. The only notable difference between lifetime and 1-year rates pertained to sexual orientation. Bisexual respondents were most likely to experience IBSA, cyberstalking, doxing, and any victimization in their lifetime. Conversely, straight respondents were least likely to be victims of IBSA, cyberstalking, any victimization, and polyvictimization. In addition, the victimization rates for those who identified as bisexual or 'other' were higher than those for gay/lesbian respondents for each TFA measure.

Table 15. Victimization Experience by Demographic Variables – Lifetime Prevalence

	Percent Experiencing Technology-Facilitated Abuse				
	IBSA	Cyberstalking	Doxing	Any Victimization	Poly-Victimization
Age					
Mean	39.6	42.2	43.0	42.8	37.5
Gender Identity (%)					
Male	5.71	5.73	3.98	12.93	2.13
Female	8.82	8.37	6.07	18.03	4.31
Other[1]	19.7	16.04	6.24	27.33	13.24
Sexual Orientation (%)					
Gay/Lesbian	15.2	9.4	3.7	22.5	5.1
Straight	6.8	6.8	5.3	14.8	3.4
Bisexual	20.0	21.5	7.9	37.9	7.7
Other	20.0	13.7	7.6	28.6	13.1
Marital Status (%)					
Married	6.1	5.2	3.9	12.3	2.2
Widowed	4.2	8.3	5.0	13.3	3.6
Divorced	7.0	11.5	8.0	22.3	4.1
Separated	14.3	14.9	6.6	27.6	5.7
Never Married	10.7	9.7	7.6	20.5	6.3
Race/Ethnicity (%)					
White	6.3	6.8	4.3	13.9	3.0
Black	7.6	10.4	5.8	18.9	3.8
Hispanic	10.1	7.2	7.6	18.9	5.2
Other	11.8	7.1	7.8	20.2	5.8
2+ Races	17.4	12.6	11.7	28.5	8.9
Education (%)					
No HS Diploma	10.9	7.6	8.5	19.3	5.9
HS/GED Diploma	6.5	7.3	5.2	15.6	3.0
Some College	6.9	8.7	6.7	17.1	4.3
Bachelor's Degree	7.2	7.6	4.2	14.7	3.4
Graduate Degree	9.5	5.2	3.4	14.5	3.1
Region (%)					
Northeast	6.1	7.0	4.9	13.9	2.84
Midwest	7.6	7.2	5.5	15.6	4.1
South	8.0	8.1	4.9	16.1	4.0
West	8.4	6.8	6.6	17.6	3.7
Household Income (%)					
< $10,000	8.8	12.0	9.4	21.4	5.9
$10,000-$24,999	7.1	12.2	7.1	20.8	4.4
$25,000-$49,999	7.8	8.8	8.1	18.7	4.7
$50,000-$74,999	6.8	9.5	5.7	16.0	5.0
$75,000-$99,999	9.9	7.0	5.1	16.9	4.3
$100,000-$149,999	7.7	5.5	4.1	15.3	1.9
> $150,000	7.0	4.5	3.5	11.8	2.8

Employment Status (%)					
Full-Time	9.0	8.4	5.3	17.6	4.4
Part-Time	9.6	9.4	7.1	18.3	5.3
Not Working	5.0	5.3	5.0	12.9	2.3

[1] Includes those identifying as transgender (n=13), nonbinary (n=15), or "other" (n=10). Due to small individual sample sizes, these categories were collapsed into a single category.

TFA Victimization by Political Ideology

Respondents who generally leaned conservative were the least likely to experience each of the five TFA measures in their lifetime (see Table 16). Liberals were most likely to experience IBSA, cyberstalking (tied with moderates), and polyvictimization, while moderates were most likely to experience doxing and any victimization. The difference in prevalence rates between conservatives and liberals was statistically significant (p<.05) for IBSA, cyberstalking, any victimization, and polyvictimization. The pattern is quite similar when examining victimization rates by political views on social issues and economic issues, except that social conservatives and economic conservatives were more likely to experience doxing relative to liberals, though the differences between these rates were quite small and not statistically significant.

Table 16. Lifetime Victimization Experience by Political Variables

	Percent Experiencing Technology-Facilitated Abuse				
	IBSA	Cyberstalking	Doxing	Any Victimization	Poly-Victimization
General Political Leaning					
Liberal	9.8	8.8	5.3	17.7	4.9
Moderate	7.7	8.8	5.9	17.8	3.8
Conservative	5.9	5.1	5.1	13.0	2.9
Social Issues					
Liberal	10.6	9.6	4.9	18.4	5.0
Moderate	7.4	7.6	5.7	16.6	3.7
Conservative	5.2	5.4	5.7	13.2	2.8
Economic Issues					
Liberal	10.5	9.0	4.2	17.8	4.3
Moderate	8.0	8.5	7.7	18.6	4.8
Conservative	6.0	5.9	4.3	13.2	2.7
Taxes					
Too Low	11.0	7.9	3.2	17.9	3.4
About Right	6.5	6.4	5.1	13.5	3.6
Too High	7.7	7.8	5.8	16.8	3.8

TFA Victimization by Mental Health Diagnoses

Finally, survey respondents were asked whether they had ever been diagnosed by a medical professional with anxiety disorder, depression, mood disorder, PTSD. As shown in Table 17, those who were diagnosed with any of the four mental health conditions were more likely to experience (or to have experienced) each of the five TFA measures, with each comparison reaching statistical significance. It is important to note, however, that these are simple correlations; we cannot infer any causality here because we do not know whether a mental health diagnosis came before or after respondents' TFA victimization.

Table 17. Lifetime Victimization Experience by Mental Health Variables

| | Percent Experiencing Technology-Facilitated Abuse | | | | |
	IBSA	Cyberstalking	Doxing	Any Victimization	Poly-Victimization
Diagnosed with anxiety disorder					
Yes	15.8	16.8	10.0	30.0	9.5
No	6.1	5.8	4.5	13.3	2.8
Diagnosed with depression					
Yes	15.2	15.0	10.3	30.3	8.1
No	6.2	6.1	4.5	13.2	3.0
Diagnosed with mood disorder					
Yes	23.2	17.9	19.7	33.7	19.8
No	7.3	7.3	5.1	15.5	3.5
Diagnosed with PTSD					
Yes	27.2	25.4	13.4	44.4	16.2
No	6.3	6.6	5.0	14.3	3.1
Diagnosed with any of these					
Yes	14.6	14.7	9.6	28.1	8.3
No	5.4	5.4	4.2	12.3	2.4

Table 18 flips the previous table and shows whether TFA victims and non-victims had been diagnosed with any of the five mental health conditions. Those who experienced each of the TFA victimization measures were more likely to have been diagnosed with all of the mental health measures. Overall, 41% of respondents who experienced TFA victimization were diagnosed with at least one of the mental health conditions, whereas 20% of non-victims had been diagnosed with any of the mental health conditions.

Table 18. Lifetime Mental Health Diagnosis by TFA Victimization

	Percent Diagnosed with a Mental Health Condition				
	Anxiety Disorder	Depression	Mood Disorder	PTSD	Any MH Condition
Experienced IBSA					
Yes	33.0	32.0	7.1	19.8	45.2
No	14.6	14.8	1.9	4.3	21.6
Experienced Cyberstalking					
Yes	35.7	31.9	5.5	18.1	45.2
No	14.4	14.8	2.1	4.4	21.6
Experienced Doxing					
Yes	29.7	30.1	8.5	13.3	41.1
No	15.2	15.3	2.0	5.0	22.4
Experienced Any Victimization					
Yes	30.1	30.6	4.9	15.2	41.1
No	13.3	13.4	1.8	3.6	20.0
Experienced Polyvictimization					
Yes	39.4	33.7	12.2	23.2	50.9
No	15.1	15.4	1.9	4.8	22.3

Harms and Costs for Victims

Financial Cost to Victims of Technology Facilitated Abuse

The survey asked victims to report on a large number of possible harms caused by their victimization. Harm categories include property value losses, moving expenses, medical and mental health care costs, technology-related costs, lost educational time and/or money, and lost workdays and earnings.

Many of these harms are qualitative (e.g., did you experience depression), while others attempt to quantify costs to the extent possible. Because some respondents were likely to be polyvictims of several types of crime, it was decided to ask the harm questions only once to respondents who indicated they were victims of at least one technology facilitated abuse. This was partly due to the fact that it would be difficult if not impossible for respondents to apportion each harm to one crime type. Because we know if each respondent was victimized by more than one crime type, in theory, this methodology would still permit a description of each crime type as well as a separate analysis of the harms to polyvictims.

In the context of a survey where respondents were not expected to spend time researching and/or documenting past losses, harms that are normally measured in dollars were expressed in ranges. For purposes of this report, ranges have been interpolated at midpoints, so that $1 to $500 is estimated to be $250; $501-$1,000 is estimated to be $750; $1,001-$5,000 is estimated to be $3,000; $5,001-$10,000 is estimated to be $7,500; $10,001-$50,000 is estimated to be $30,000, and $50,000 or more is estimated to be $75,000. To the extent losses far exceed $75,000, the cost estimates presented here are conservative. However, instances where individuals responded that their costs were $50,000 or more were rare. For example, only two out of 94 polyvictims indicated their moving costs exceeded $50,000. In a small percentage of cases, respondents indicated they incurred a cost but answered "don't know" when asked for an estimate of that cost category. Those cases have been estimated at the mean cost for others in that victimization-cost category.

The following tables are based on the weighted sample of 403 victims – 132 of whom were IBSA victims, 66 doxing victims, 111 stalking victims, and 94 polyvictims who reported more than one type of victimization. These four categories are mutually exclusive so that, for example, a polyvictim who was both a doxing and cyberstalking victim would only be counted as a polyvictim. In contrast, the "All Victims" category is based on the full sample of 403 victims. This section focuses on harms that were either expressed in dollar values or where we were able to estimate dollar costs from the nature of the responses. The actual questions used to estimate dollar values are identified in [BRACKETS], e.g., [HARM110_D] refers to the question in the survey "About how much was the value of the property that was destroyed or vandalized?"

Costs are always reported as the average cost for all victims in their respective crime category as well as for all victims combined—even though some victims did not experience that harm. For example, as shown in the first row of Table 19, the average property value loss for all 403 victims was $925 dollars (95% CI $322-$1,528). However, only 11.7% of victims incurred quantifiable property value losses—with the average loss being $7,864 (95% CI $2,996-$12,732). Finally, the maximum loss reported in our sample was a property value loss of $75,000 (actually "$50,000 or more" as noted above). The overall victim average is useful for estimating the overall cost of victimization, while the average cost per victim who experienced that harm is useful in better understanding the distribution of harms and the potential needs for some of the most harmed victims.

Property Value Losses

As shown in Table 19, about 11.7% of all victims incurred property value costs such as destroyed or vandalized property [HARM110_D]. Polyvictims suffered the highest losses—$2,710 per victim or $12,724 for the 21.3% of victims who incurred these losses.

Table 19. Property Value Losses to Victims of TFA

	N	Ave Cost (all victims)	95% CI	Percent reporting > $0	Average Cost (victims > $0)	95% CI	MAX
All victims	403	$925	$322-1,528	11.7%	$7,864	$2,996-12,732	$75,000
IBSA	132	$101	($9)-210	7.1%	$1,412	($267)-3,093	$7,500
Doxing	66	$326	(-$0.5)-652	12.7%	$2,532	$591-4,477	$7,500
Cyberstalking	111	$746	(-$9)-1,500	9.3%	$8,745	$711-16,778	$30,000
Polyvictim	94	$2,710	$288-5,133	21.3%	$12,724	$1,702-23,745	$75,000

Moving Expenses

Table 20 reports on moving costs to victims who reported they moved as a result of their victimization [HARM110_F]—including such costs as hiring movers, breaking a lease, or costs incurred from buying and/or selling a home. These are relatively rare outcomes—about 8.9% of victims overall reported incurring such expenses. However, 17.1% of polyvictims reported an average moving expense of $29,803 (95% CI $12,639-$46,997). Note that the estimated cost for all victims as well as all victims who incurred moving expenses is highly variable and the 95% confidence intervals cross zero. This is largely due to the fact that the largest number of victims were subject to IBSA—and they are also the group that are least likely to incur moving expenses.

Table 20. Moving Expenses Incurred by Victims of TFA

	N	Ave Cost (all victims)	95% CI	Percent reporting > $0	Average Cost (victims > $0)	95% CI	MAX
All victims	403	$3,769	($40)-7,578	8.9%	$42,909	($40)-7,578	$30,000
IBSA	132	$217	($166)-600	4.8%	$4,549	($7,399)-16,496	$3,000
Doxing	66	$157	(-$27)-342	6.6%	$2,398	$850-$3,945	$7,500
Cyberstalking	111	$242	($13)-472	7.8%	$3,114	$868-5,360	$30,000
Polyvictim	94	$5,098	$1,466-8,731	17.1%	$29,803	$12,639-46,997	$75,000

Mental Health Costs

Table 21 reports on the out-of-pocket mental health-related costs incurred by victims [HARM210_F]. As shown, the average dollar costs are relatively small on a per-victim basis. However, because only about 10-15% of victims incurred such costs, the average out-of-pocket costs to those who do incur mental health care costs is significant. Victims of IBSA who incurred such costs report an average of $7,395 (CI $1,711 to $13,078), while the average for polyvictims who incur these costs is $5,840 with the maximum being reported to be over $50,000 (shown here as an estimated $75,000).

90

Additional follow-up questions were asked of those who incurred out-of-pocket costs to determine if additional mental health care costs were covered by other sources such as health insurance, family members, or victim assistance programs [HARM220_F], and whether the victim was still receiving mental health care due to victimization [HARM230_F]. Approximately 48.7% of victims receiving mental health care reported that additional costs were covered by these other sources, and 38% reported that their treatment was still underway as of the date of the survey. Thus, out-of-pocket costs will ultimately be higher than the figures shown in Table 21, and third-party costs are not accounted for in these estimates.

Table 21. Mental Health Expenses Incurred by Victims of TFA

	N	Ave Cost (all victims)	95% CI	Percent reporting > $0	Average Cost (victims > $0)	95% CI	MAX
All victims	403	$567	$271-863	10.7%	$5,313	$2,849-7,777	$75,000
IBSA	132	$748	$108-1,389	10.1%	$7,395	$1,711-13,078	$18,382
Doxing	66	$15	(-7)-38	3.3%	$470	($2,662)-3,603	$750
Cyberstalking	111	$343	$59-626	10.7%	$3,178	$957-5,399	$8,233
Polyvictim	94	$964	$120-1,007	16.5%	$5,840	$711-10,969	$75,000

Physical Health Costs

Table 22 reports on the out-of-pocket physical health-related costs incurred by victims [HARM210_H]. As shown, the average dollar costs are relatively small on a per-victim basis. However, because only about 10-15% of victims incurred such costs, the average out-of-pocket costs to those who do incur health care costs is significant. Victims of IBSA who incurred such costs report an average of $8,791 (CI $855 to $16,727), while the average for polyvictims who incur these costs is $13,566 (CI $1,873 to $25,259) with the maximum being reported to be over $50,000 (shown here as an estimated $75,000).

Additional follow-up questions were asked of those who incurred out-of-pocket costs to determine if additional health care costs were covered by other sources such as health insurance, family members, or victim assistance programs [HARM220_H], and whether the victim was still receiving health care due to victimization [HARM230_H]. Approximately 51.9% of victims receiving health care reported that additional costs were covered by these other sources, and 38.4% reported that their treatment was still underway as of the date of the survey. Thus, out-of-pocket costs will ultimately be higher than the figures shown in Table 22, and third-party costs are not accounted for in these estimates.

Table 22. Physical Health Expenses Incurred by Victims of TFA

	N	Ave Cost (all victims)	95% CI	Percent reporting > $0	Average Cost (victims > $0)	95% CI	MAX
All victims	403	$681	$227-1,135	8.3%	$8,172	$2,980-13,364	$75,000
IBSA	132	$506	$2-1,010	5.8%	$8,791	$855-16,727	$17,250
Doxing	66	$53	(-53)-159	1.8%	$3,000	---	$3,000
Cyberstalking	111	$81	$14-148	9.4%	$866	$275-1,455	$3,000
Polyvictim	94	$2,072	$249-3,895	15.3%	$13,566	$1,873-25,259	$75,000

Technology-Related Costs

The survey asked several questions about technology-related costs incurred such as closing accounts and/or opening new accounts on apps or websites, and purchasing new or replacement phones, tablets, computers or other devices. As a prelude to those questions, however, several questions were asked about the impact of victimization on their use of technology [HARM_300]. As shown in Table 23, 42% of all victims reported closing accounts, while 31.1% opened new accounts. 14.3% reported that they had been locked out of devices or accounts, while 40.6% indicated that they felt nervous or frightened using existing accounts. Finally, 18.8% reported purchasing new phones, tablets or other devices, and 8.9% bought smart home devices such as security systems.

Table 23. Technology-Related Expenses Incurred by Victims of TFA

	N	Closed accounts	Opened accounts	Locked out of devices or accounts	Felt nervous or frightened using existing accounts	Bought new phone, tablet, etc.	Bought new smart home device (e.g., security system)
All victims	403	42.0%	31.1%	14.3%	40.6%	18.8%	8.9%
IBSA	132	26.9%	15.2%	5.6%	28.6%	9.0%	2.0%
Doxing	66	42.1%	32.7%	11.0%	29.2%	16.7%	16.3%
Cyberstalking	111	56.3%	41.6%	16.2%	48.1%	23.3%	8.5%
Polyvictim	94	47.4%	39.6%	26.7%	55.6%	29.0%	14.4%

Table 24 reports on the estimated costs to those who reported they had spent money to close or open new accounts [HARM310_AB] and/or to purchase new devices [HARM310_EF] as indicated above. As shown, the average cost over all victims was $985 (CI $301 to $1,669), while the average cost for those who reported any such costs was $3,443 (CI $1,084 to $5,802).[7]

---

[7] One polyvictim reported spending over $50,000 in both categories (e.g., opening/closing accounts and buying new devices/security systems); hence their entry was coded as $150,000 ($75,000 each). Ignoring that one outlier reduces

Table 24. Technology-Related Expenses Incurred by Closing or Opening New Accounts

	N	Ave Cost (all victims)	95% CI	Percent > $0	Ave Cost (victims > $0)	95% CI	MAX
All victims	403	$985*	$301-1,669	28.6%	$3,443*	$1,084-5,802	$150,000
IBSA	132	$306	$79-533	13.5%	$2,262	$778-3,745	$10,500
Doxing	66	$808	$324-1,291	32.7%	$2,469	$1,372-3,565	$7,500
Cyberstalking	111	$472	$242-703	33.4%	$1,416	$827-2,006	$6,000
Polyvictim	94	$2,663*	($240)-5,566	41.3%	$6,454*	($627)-13,537	$150,000

* See footnote 6 for alternative estimates ignoring one outlier.

Impact on Education

Table 25 reports on the frequency of school-related harms for all victims. However, many victims were well beyond school age when the offense took place [HARM400]. Table 26 replicates these results restricting the sample to respondents who indicated that they were a student at any time when they experienced victimization. These restrictions result in 82 victims – or 99 when weighted – representing about 25% of our victim sample. Of those victims who were in school at some point while being victimized, 37.1% reported missing some days from school, 4.4% reported dropping out and 2% reported being expelled from school.

Table 25. Percent of Victims of TFA Experiencing Difficulty in School

	N	Hard time focusing	Took extended break	Dropped out of school	Expelled from school	Punished at school	Missed days from school	Images shared in school community	Any[1]
All victims	403	15.8%	3.5%	1.1%	0.5%	2.2%	9.1%	4.2%	9.5%
IBSA	132	13.8%	1.4%	---	---	2.1%	5.6%	3.5%	6.0%
Doxing	66	3.9%	3.9%	---	---	--	3.9%	--	3.9%
Cyberstalking	111	13.8%	3.7%	1.2%	---	--	8.4%	--	8.4%
Polyvictim	94	29.2%	5.8%	3.1%	2.1%	6.2%	18.4%	13.1%	17.4%

[1] Rows do not add up because some victims reported multiple events.

---

the average cost for polyvictims to $1,269 (CI $442 to $2094) and the average cost for all victims to $657 (CI $429 to $887). For those that report positive losses, these figures would be $3,117 (CI $944 to $1,198) and $2,311 (CI $1,596 to $3,026) respectively.

Table 26. Percent of Students Who Were TFA Victims Experiencing Difficulty in School

	N	Hard time focusing	Took extended break	Dropped out of school	Expelled from school	Punished at school	Missed days from school	Images shared in school community	Any[1]
All victims	99	64.6%	14.2%	4.4%	2.0%	8.9%	37.1%	17.2%	67.4%
IBSA	32	56.5%	5.9%	---	---	8.8%	22.8%	14.5%	56.5%
Doxing	3	100%	100%	---	---	--	100%	--	100%
Cyberstalking	23	67.3%	18.2%	6.1%	---	--	40.9%	--	67.3%
Polyvictim	41	67.2%	13.2%	7.2%	4.8%	14.3%	42.2%	30.1%	73.9%

[1] Rows do not add up because some victims reported multiple events.

Table 27 reports on the average number of school days lost due to victimization [HARM410_B]. These figures are averaged over all victims – including those not in school at the time of the offense. Table 28 restricts the analysis to those who reported they were in school when the victimization occurred. The average student who is a victim of TFA missed 6.2 days of school; however, only 37.1% of student victims missed school days. For those who did miss school days, the average was 16.6 days.

Table 27. School Days Lost by Victims of TFA

	N	Ave # Days if missed	% Miss days from school	Ave # Days over all victims	95% CI	Max Days
All victims	403	16.6	8.9%	1.5	0.6-2.4	100
IBSA	132	7.1	5.6%	0.4	0.001-.8	14
Doxing	66	30	3.9%	1.2	(1.1)-3.5	30
Cyberstalking	111	23.6	8.4%	2.0	(0.5)-4.4	100
Polyvictim	94	14.9	18.4%	2.8	0.6-4.9	80

Table 28. School Days Lost by Students Who Were TFA Victims

	N	Ave # Days if missed*	% Miss days from school	Ave # Days over all student victims	95% CI	Max Days
All victims	99	16.6	37.1%	6.2	2.6-9.8	100
IBSA	32	7.1	22.8%	1.6	0.1-3.1	14
Doxing	3	30	100%	---	---	30
Cyberstalking	23	23.6	40.9%	9.6	(2.8)-22	100
Polyvictim	41	14.9	42.2%	6.3	1.4-11.2	80

* Note: This column is identical to that in Table 25 because all victims who missed days in school were, by definition, in school at the time of the victimization.

94

Some students who were victims of TFA crimes also lost tuition or other fees due to dropping out for one or more courses [HARM410_CDE]. Table 29 averages these losses over all victims, while Table 30 averages them over victims who were students at the time of the offense. Approximately 12.7% of students who were victimized reported losing tuition fees. The largest loss in the sample was $3,000. For those who lost tuition, the average loss was $794.

Table 29. Lost School Tuition/Fees Incurred by Victims of TFA

	N	Ave Cost (all victims)	95% CI	Percent > $0	Average Cost (victims > $0)	95% CI	MAX
All victims	403	$24	$1-48	3.1%	$794	$104-1,483	$3,000
IBSA	132	$4	($1.7)-8.9	0.5%	$250	---	$250
Doxing	66	$27	($26)-81	3.9%	$692*	---	$692
Cyberstalking	111	$8	($1.2)-18	3.7%	$224	$108-339	$250
Polyvictim	94	$72	($22)-166	4.1%	$2,634	($1,790)-7,059	$3,000

* Because the sole victim of doxing who indicated they lost school fees did not know the amount, we estimated losses based on the average loss of all victims who reported a dollar loss related to lost school fees.

Table 30. Lost School Tuition/Fees Incurred by Students Who Were Victims of TFA

	N	Ave Cost (all victims)	95% CI	Percent > $0	Average Cost (victims > $0)	95% CI	MAX
All victims	99	$101	$5-197	12.7 %	$794	$104-1,483	$3,000
IBSA	32	$15	($7.8)-37.2	5.9%	$250	---	$250
Doxing	3	$692*	---	3.9%	$692*	---	$692
Cyberstalking	23	$41	($6.8)-88	18.2%	$224	$108-339	$250
Polyvictim	41	$164	($56)-385	9.5%	$2,634	($1,790)-7,059	$3,000

* Because the sole victim of doxing who indicated they lost school fees did not know the amount, we estimated losses based on the average loss of all victims who reported a dollar loss related to lost school fees.

Employment Disruptions and Lost Earnings

Respondents who were victims of at least TFA were asked several questions about any work-related harms [HARM500]. As shown in Table 31, 21.6% of all victims reported they had a hard time focusing on their work—with polyvictims having the highest rate of 35%. About 12.9% of victims missed some work—either paid or unpaid. The rates were significantly higher for stalking (15.3%) and polyvictims (22.7%) compared to victims of IBSA (7.8%) and Doxing (5.4%). Similarly, about 7.9% reported they were either fired or quit their jobs. In addition, about 5.3% reported that they had turned down a promotion or missed a job opportunity they otherwise thought they would have been able to obtain. Overall, 26.4% of all victims suffered at least one of these job-related harms—with the rate for polyvictims being 41.8%.

95

Since not all victims were working at the time of the offense, additional tables restricted the sample to only those who reportedly were "employed at any time" when they experienced the victimization. Note that of the 403 (weighted) victims, 230 were working, 99 were in school and 74 reported neither. Of the 230 working victims, 43 were also in school at some time during their victimization. Thus, some of the respondents are included in both the tables restricted to students and those restricted to the employed. (Note that about 11% of victims were over 65; thus, in addition to retired, some were likely unemployed, disabled, or homemakers.)

As shown in Table 32, 37.6% of employed victims reported having difficulty focusing on their jobs, 21.9% missed days at work, 13.0% quit or were fired from their jobs, and 9.1% reported they missed out on promotions or other job opportunities.

Table 31. Employment Disruptions to Victims of TFA

	N	Hard time focusing on job	Missed days (paid)	Missed days (unpaid)	Family Member Missed Days	Quit or fired	Turned down for promotion or missed job opp.	Personal info or images shared with coworkers	Any[1]
All victims	403	21.6%	6.7%	7.8%	4.1%	7.9%	5.3%	6.2%	26.4%
IBSA	132	16.3%	5.2%	4.4%	---	1.8%	1.8%	1.7%	17.6%
Doxing	66	14.1%	5.4%	2.1%	---	5.8%	1.3%	8.6%	19.9%
Cyberstalking	111	21.0%	7.3%	8.2%	2.8%	11.7%	5.3%	---	27.8%
Polyvictim	94	35.0%	9.0%	16.2%	14.2%	13.2%	12.8%	17.9%	41.8%

[1] Rows do not add up because some victims reported multiple events.

Table 32. Employment Disruptions to Employed Victims of TFA

	N	Hard time focusing on job	Missed days (paid)	Missed days (unpaid)	Family Member Missed Days	Quit or fired	Turned down for promotion or missed job opp.	Personal info or images shared with coworkers	Any[1]
All victims	232	37.6%	11.6%	13.6%	6.4%	13.0%	9.1%	10.7%	45.3%
IBSA	74	28.9%	9.3%	7.8%	---	3.2%	3.2%	3.1%	31.3%
Doxing	38	24.6%	9.4%	3.7%	---	10.0%	2.4%	15.0%	34.7%
Cyberstalking	63	36.9%	12.9%	14.4%	2.5%	18.3%	9.3%	---	46.5%
Polyvictim	57	58.2%	15.0%	27.0%	23.5%	22.0%	21.2%	29.7%	69.4 %

[1] Rows do not add up because some victims reported multiple events.

Table 33 reports on the estimated number of lost workdays – both paid [HARM510_C] and unpaid [HARM510_D]—for victims of TFA. This is averaged over all victims, regardless of their employment status at the time of victimization. The value of paid and unpaid time off was estimated based on the average wage rate for all employees in the U.S.[8] Paid work loss is estimated to be $214 per victim, with an additional $415 in unpaid time off. The average polyvictim suffers $1,442 in unpaid time off the job.

Table 33. Cost of Lost Workdays While Employed for Victims of TFA

	N	Mean days missed work (paid)	Max days missed work (paid)	Mean days missed work (unpaid)	Max days missed work (unpaid)	Estimated value of paid work loss	Estimated value of unpaid work loss
All victims	403	0.82	120	1.59	365	$214	$415
IBSA	132	0.30	15	0.28	20	$78	$73
Doxing	66	0.23	10	0.22	12	$60	$57
Cyberstalking	111	0.68	60	0.61	20	$177	$159
Polyvictim	94	2.12	120	5.52	365	$554	$1,442

Table 34 replicates this analysis with the subsample of victims who reported they were employed at any time when they were victimized. As shown, the earnings loss to victims can be considerable. The average estimated unpaid earnings loss to all employed victims was $5,748 and $9,641 to polyvictims. Of course, as shown in Table 31, only 13.6% of all victims and 27.0% of polyvictims missed unpaid days at work. Thus, the cost to those who *do* incur unpaid lost workdays is considerably higher. In fact, one victim reported 365 days unpaid leave before quitting his job and being unemployed for another 900 days. The estimated loss of 365 days income is $95,367.[9] Although an outlier, the second largest unpaid workdays was reported to be 120 days, valued at approximately $31,353.

---

[8] Although the survey asked victims to report on the dollar value of lost workdays, due to a survey programming error, this variable (HARM520_C) is unusable. Thus, the dollar value of both paid and unpaid time off work was estimated based on the average hourly earnings for US workers, $32.66 (BLS Average hourly earnings, October 2022, https://www.bls.gov/news.release/empsit.t19.htm.

[9] This loss is plausible if not conservative. This individual is a 57-year-old male with a master's degree and now reports household income in excess of $150,000 annually.

Table 34. Cost of Lost Workdays While Employed to Employed Victims of TFA

	N	Mean days missed work (paid)	Max days missed work (paid)	Mean days missed work (unpaid)	Max days missed work (unpaid)	Estimated value of paid work loss	Estimated value of unpaid work loss
All victims	232	1.43	120	22.0	365	$374	$5,748
IBSA	74	0.53	15	6.5	20	$138	$1,698
Doxing	38	0.41	10	10.4	12	$107	$2,717
Cyberstalking	63	1.20	60	8.7	20	$314	$2,273
Polyvictim	57	3.52	120	36.9	365	$920	$9,641

In addition to temporary time taken off work, about 6.7% of victims reported quitting or being fired from their jobs. In these cases, victims were asked to estimate the number of days they were unemployed before obtaining a new job [HARM510_FG]. Table 35 estimates lost income to victims who ultimately quit or were fired from their jobs—once again using the average hourly earnings in the U.S. to value days off the job. Averaged over all victims (regardless of whether they were employed at the time), lost earnings due to unemployment is estimated to be $2,900—ranging from a low of $470 for IBSA to a high of $7,629 for polyvictims. Restricting the analysis to victims who were employed at the time of victimization, these figures increase to $5,017 for the average victim with the largest loss being $12,698 for polyvictims. Because only a small percentage of victims suffer job losses (about 7.5% of all victims and 13% of all employed victims), these average figures do not fully account for the impact on victims who do suffer periods of unemployment. Thus, restricting the analysis to only those victims who experienced unemployment, the average period of unemployment is 141 days at an estimated loss of $36,866 per unemployed victim. The average period of unemployment for a polyvictim who is unemployed is 220.6 days, or $57,638.

Table 35. Lost Income Due to Job Loss (Quit or Fired)

	N	Averaged over all victims		Averaged over all employed victims		Averaged over all employed victims who suffered loss		
		Days missed while unemployed	Estimated Loss per victim[1]	Days missed while unemployed	Estimated Loss per victim[1]	Days missed while unemployed	Estimated Loss per victim[1]	Max number of days out of work
All victims	403	11.1	$2,897	19.2	$5,017	147.9	$38,636	900
IBSA	132	1.8	$470	3.3	$861	102.8	$26,861	180
Doxing	66	12.2	$3,184	21.3	$5,563	212.2	$55,441	700
Cyberstalking	111	6.0	$1,562	10.2	$2,676	51.0	$13,327	180
Polyvictim	94	29.2	$7,641	48.6	$12,686	249.5	$65,200	900

Note: These losses are in addition to those incurred while on unpaid leave that are included in Tables MC-15 and MC-16 above. It is possible that these costs were partly offset by unemployment insurance or other social welfare benefits.

Overall, about 4.2% of victims reported that after losing or quitting their jobs, they ended up in a lower paying position [HARM520_FG]. Respondents were asked how much less per month they made in their new job [HARM530_FG], and whether this figure was gross (before taxes and deductions) or take-home pay (after taxes and deductions) [HARM540_FG]. Table 36 estimates the monthly loss averaged over all victims to be $84, but $1,992 averaged over victims who suffered a job loss. Although some workers might quickly move into other jobs or obtain promotions that increase their wages to pre-victimization levels, others might suffer a permanent wage shock. Table 36 provides a conservative estimate of losses based on one year of lower earnings. Thus, the average victim who moves to a lower paying job suffers $23,901 in lower earnings in one year. IBSA victims and polyvictims suffer the largest such loss, $38,068 and $46,396 respectively.

Table 36. Lost Income Due to Moving to Lower Paying Job

	N	% with loss	Averaged over all victims		Including only victims who suffered job loss:			
			Monthly income	Long-term (1-year)	Monthly income	Long-term (1-year)	Max (monthly)	Max (1-year)
All victims	403	4.2%	$84	$1,012	$1,992	$23,901	$9,975	$104,490
IBSA	132	1.8%	$57	$686	$3,172	$38,068	$3,483	$41,796
Doxing	66	2.9%	$55	$661	$1,868	$22,415	$3,000	$36,000
Cyberstalking	111	7.6%	$56	$678	$741	$8,892	$3,483	$41,796
Polyvictim	94	4.6%	$175	$2,105	$3,866	$46,396	$8,708	$104,490

Note: Respondents were asked if their estimated monthly income loss was before or after tax. Losses identified by the respondent to be "after-tax" were increased based on an average tax rate of 13.8%.[10]

Total Financial Cost of Victimization

Table 37 adds up all the out-of-pocket financial costs identified through the survey. Costs that are borne by insurance companies, governments and non-profits are not included in this table. Property costs include vandalized property, moving costs, and the cost associated with replacing accounts or devices. Medical and mental health costs include all reported out-of-pocket costs as of the date of the survey. Earnings losses include the cost of lost tuition, unpaid leave, and reduced wages for the first year upon moving to a new job. As indicated above, some of the estimated earnings losses might have been partially offset by unemployment insurance benefits.

The average financial cost to victims of technology-facilitated abuse is estimated to be $8,874 (CI $4,849 - $12,902). The average cost for IBSA is estimated to be $3,113; $5,332 for doxing, $4,264 for stalking. The largest crime costs fall upon polyvictims, with average costs of

---

[10] According to US Census data, median household income was $74,580 in 2022, with after-tax income being $64,240. https://www.census.gov/library/publications/2023/demo/p60-279.html (Tables A-1 and B-1). Thus, average state and federal income taxes were 13.8%. To account for this, earning losses that were reported after-tax were increased by 16.1%. This is conservative as it does not include the full value of employee-paid benefits. According to OECD data, the average take-home pay after taxes and benefits in the U.S. was approximately 30%. https://www.oecd.org/tax/tax-policy/taxing-wages-united-states.pdf

$28,848 (95% CI $8,965 - $40,731). All the estimates in Table 37 are conservative as they represent out-of-pocket costs as of the date of the survey – and many respondents reported continued medical and/or mental health costs and lost earnings into the future that are not estimated in this report. They are also limited to the victim's out-of-pocket losses and thus exclude costs incurred by family or friends as well as all third-party costs.

Table 37. Total Financial Costs Borne by Victims of TFA

	N	Property	Medical	Mental Health	Earnings	**Combined**	95% CI	Max
All victims	403	$3,266	$681	$567	$4,539	**$8,874**	$4,849-$12,902	$649,857
IBSA	132	$624	$506	$748	$1,234	**$3,113**	$451 - $5,775	$147,576
Doxing	66	$1,290	$53	$15	$3,972	**$5,332**	($1,197) – 11,861	$199,345
Cyber stalking	111	$1,461	$81	$343	$2,379	**$4,264**	$1,639-$6,887	$89,576
Poly victim	94	$10,472	$2,072	$964	$11,340	**$24,848**	$8,965-$40,731	$649,857

Table 38 examines the distribution of financial costs of TFA victimization by household income in more detail. As shown, the average cost of victimization is highest at the lowest household income levels—$47,205 at income less than $10,000 annually and $15,996 at household income between $10,000 and $25,000. These figures compare to the overall average of $8,874. However, median losses for those who suffer any financial losses do not differ significantly across household income. There are two reasons for this large difference. First, as shown, victims in lower income households are more likely to incur financial costs (63.9% to 70.6% for the lowest income categories, compared to 40.0% overall). Second, they are more likely to be fired or quit their jobs following victimization (13.9% to 17.6% versus overall average of 7.6%). More details on the financial costs of TFA victimization are presented below.

Table 38. Comparison of Costs by Household Income

	Average cost	Percent with costs > 0	Average for costs > 0	Median for costs > 0	Max	Fired or quit job
< $10k	$47,205	70.6%	$66,873	$3,533	$649,857	17.6%
$10k - $25k	$15,996	63.9%	$25,038	$3,000	$199,345	13.9%
$25k - $50k	$9,599	46.7%	$20,569	$1,000	$153,000	6.7%
$50k - $75k	$6,024	40.0%	$15,453	$7,933	$65,834	6.8%
$75k - $100k	$6,023	34.5%	$17,434	$3,500	$190,734	9.1%
$100k - $150k	$5,620	22.8%	$24,641	$3,385	$112,500	10.5%
> $150k	$6,300	33.3%	$18,900	$1,133	$429.652	1.2%
All income levels	$8,874	40.0%	$23,787	$3,000	$649,857	7.6%

Minor victims

As stated above, for the purposes of this report, we have estimated the number of minors by assuming the following were victimized when they were minors:

(1) All 18-year-old victims at the time of the survey
(2) All 19- and 20-year-old victims who indicated they became aware of their victimization more than 12 months prior to the survey (i.e. before November 2021), and
(3) All 21-year-old victims who indicated they became aware of their victimization prior to March 2020.

The result was that out of the 403 (weighted) victims, 53 (13.1%) were identified as likely to have been victimized when they were minors. This small sample makes comparisons difficult—especially once breaking the sample down by crime type. However, overall, the average combined financial costs of minor victims were estimated to be $2,743 (95% CI $125 - $5,612). In contrast, the average financial costs to the 360 non-minors were estimated to be $9,799 (95% CI $5,193 - $14,405).

Severity of Victim Impacts

Although most of the tables represent average and ranges of estimated impacts, TFA impacts at the extreme can be devasting to individual victims. To illustrate this, we examined the profile of two respondents who reported victimizations resulting in several of the largest dollar losses.

Victim #1 (CaseID 2175795) was a 33-year-old White, non-married female with a bachelor's degree or higher, who reported being victimized by both doxing and stalking. The doxing incident occurred pre-Covid, while she became aware of the stalking incident more recently (within the past 12 months). Both were perpetrated by strangers. The stalking included repeated contacts through email/social media/phone, installation of tracking technology, and even the impersonation of the victim to interfere with her personal or work relationships. The victim was employed at the time and also had a small business.

Because harms are not always separable by crime, respondents were asked about their harms without necessarily identifying which (or both) offenses were the primary cause. Victim #1 reported that she suffered from physical ailments such as headaches and lack of sleep and was still being treated by a physician years after her victimization. She estimated her own out-of-pocket costs (aside from that paid by insurance) was over $50,000. She reportedly took about 4 months off work on paid leave and then an additional 4 months unpaid before quitting her job. She was unemployed for a year and her next job paid her more than $5,000 monthly less (after taxes) than she earned previously. She also reportedly missed out on another job opportunity that would have likely paid $5,000+ monthly than she was earning in her previous job. Finally, she also reportedly spent more than $50,000 on legal fees in addition to significant time and money trying to remedy the many problems resulting from her victimization. Overall, her total financial costs have been estimated to exceed $480,000.

Victim #2 (CaseID 4005001) is a 45-year-old White married female with a high school degree. She was the victim of IBSA when she was 35. The offender was her partner at the time who took photos of her without her knowledge or consent. She was also independently a victim of cyberstalking by a different partner. Victim #2 reported that she was working and also was a student at the time of one or both incidents. She developed a substance abuse problem and suffered from depression. She reportedly missed a week of work and then quit her job. She reportedly was unemployed for more than 2 years. Overall, her total financial costs have been estimated to be nearly $200,000. In both cases, future costs are likely to be higher.

Regression Analysis of Victimization Costs

Regression analysis on the combined cost of victimization was performed with both a linear and log-linear specification (with the dependent variable being the natural log of Combined Costs + 1). Due to the skewness of victimization costs, the log-linear specification was a better fit, as shown in the following two tables. The only significant explanatory variables were polyvictimization (positive), household income (negative) and two of the age variables – with higher costs being found for the middle age categories of 30-44 and 45-59 (compared to under 30 and 60+ age categories).

Table 39. Linear Regression – Combined Costs

	Coef.	Std. Error	t	p	95% CI	
Abuse Type[a]						
Doxing Only	2910.07	3989.00	0.73	.466	-4940.44	10760.58
Cyberstalking Only	821.44	2896.60	0.28	.777	-4879.17	6522.06
Polyvictimization	22448.55	7706.61	2.91	**.004**	7281.65	37615.44
When Occurred						
Past 12 Months	1386.34	6019.69	0.23	.818	-10460.65	13233.32
> 12 months, before COVID	7017.23	7443.83	0.94	.347	-7632.51	21666.97
Pre-COVID	---	---	---	---	---	---
Sex (1=Female)	-11963.81	8009.45	-1.49	.136	-27726.70	3799.09
Race/Ethnicity[b]						
Black, Non-Hispanic	-5379.43	8449.41	-0.64	.525	-22008.19	11249.33
Other, Non-Hispanic	-3719.49	7146.74	-0.52	.603	-17784.55	10345.57
Hispanic	-8480.72	6609.69	-1.28	.200	-21488.83	4527.39
2+ Race, Non-Hispanic	2906.65	9170.93	0.32	.752	-15142.10	20955.40
Suburban Residence	7314.50	6165.99	1.19	.236	-4820.40	19449.40
Household Income	-55.53	44.71	-1.24	.215	-143.53	32.47
Kids	4087.99	5469.06	0.75	.455	-6675.32	14851.31
Age Category[c]						
30-44	15049.36	7119.12	2.11	**.035**	1038.66	29060.05
45-59	10296.27	5030.58	2.05	**.042**	395.89	20196.65
60+	3722.24	4423.69	0.84	.401	-4983.75	12428.23
Constant	5147.77	4423.69	0.84	.401	-4983.75	12428.23

R^2	0.086	

[a] Reference category is IBSA Only.
[b] Reference category is White, Non-Hispanic.
[c] Reference category is 18-29.

Table 40. Linear Regression – Natural Log of Combined Costs + 1

	Coef.	Std. Error	t	p	95% CI	
Abuse Type[a]						
Doxing Only	1.34	0.79	1.69	.091	-.22	2.90
Cyberstalking Only	1.31	0.70	1.86	.064	-.08	2.69
Polyvictimization	2.86	0.74	3.87	**.000**	1.41	4.31
When Occurred						
Past 12 Months	1.49	1.85	0.81	.419	-2.14	5.12
> 12 months, before COVID	1.33	2.39	0.56	.577	-3.37	6.03
Pre-COVID	---	---	---	---	---	---
Sex (1=Female)	-0.07	0.53	-0.14	.889	-1.12	.97
Race/Ethnicity[b]						
Black, Non-Hispanic	-0.11	0.83	-0.13	.898	-1.75	1.54
Other, Non-Hispanic	-0.86	1.04	-0.83	.409	-2.90	1.18
Hispanic	0.09	0.70	0.13	.895	-1.28	1.47
2+ Race, Non-Hispanic	0.74	0.99	0.75	.457	-1.21	2.69
Suburban Residence	0.29	0.50	0.57	.569	-.70	1.28
Household Income	-0.01	0.00	-3.07	**.002**	-.01	-.00
Kids	0.78	0.59	1.33	.185	-.37	1.93
Age Category[c]						
30-44	1.36	0.71	1.91	.057	-.04	2.76
45-59	1.57	0.68	2.33	**.020**	.25	2.90
60+	0.29	0.77	0.37	.711	-1.23	1.80
Constant	1.65	0.84	1.96	.051	-.01	3.31
R^2	0.123					

[a] Reference category is IBSA Only.
[b] Reference category is White, Non-Hispanic.
[c] Reference category is 18-29.

Distribution of Costs

The survey data reveal an important distributional impact of victimization. As noted in the regression analyses, costs are negatively related to household income—suggesting that the financial burden of TFA falls disproportionately on lower income households. In fact, it appears that this pattern is also evident in the risk of victimization itself. As shown in the previous regression analyses, the likelihood of victimization decreases with household income. It is also lower for those age 30+ (much lower for those aged 60+) and higher for females and those identifying as being mixed race.

Willingness to Pay for Crime Reduction

All survey respondents were asked a series of questions designed to elicit their willingness-to-pay to reduce the risk of each of the three TFA crimes in this study. After defining each crime and describing typical victim harms, respondents were given a combination of crime reductions as well as costs and asked to choose their preferred outcome (including the status quo which would cost zero). This discrete choice experiment followed normal protocols as described in the Methods for Cost Analysis section above. Although each respondent was asked about all three crimes, their order was randomly assigned. The options were to choose a 50% reduction, 25% reduction or no reduction (status quo), with randomly assigned annual household costs of $50, $100, $250, $500, and $1,000—although the status quo was always set at zero costs. Ordering was preserved so that a 50% reduction always cost more than a 25% reduction. For example, the following text was provided for cyberstalking:

… **cyberstalking** is when someone uses technology to repeatedly harass another person, stalk them, or monitor their activity.

- *About 3,200 out of every 100,000 U.S. adults (3.2%) have experienced cyberstalking in the past year.*

- *People who experience cyberstalking often alter their daily routines, feel at risk no matter where they are, feel psychological distress or fear, and have stress-related health problems. They also may have expenses related to closing and opening new accounts, paying for therapy, improving home security, and replacing electronic devices like their phone.*

Your state government is considering the adoption of **cyberstalking** reduction programs that have proven to be successful in other states. ***Ignore who pays for these programs directly. Instead, think about the amount the average household should actually pay for the program – regardless of whether this is through taxes, consumer prices, or lower shareholder profits***.

Which of these programs would you support?

1. *Program A cuts cyberstalking from 3,200 to 1,600 per 100,000 (**50% decrease**) and would cost your household **$250** per year.*

2. *Program B cuts cyberstalking from 3,200 to 2,400 per 100,000 (**25% decrease**) and would cost your household **$100** per year.*

3. ***Do nothing** – cyberstalking would remain at 3,200 per 100,000 adults. This would cost your household **$0** per year.*

Table 41 reports on the percentage of respondents who were willing to pay more than zero for the stated crime reduction-price bundle. As shown, between 35-38% of respondents were willing to pay for some crime reductions.[11] Thus, between 62% and 65% of respondents preferred the status quo and were not interested in paying for additional crime reductions.

Respondents were asked to explain their choices with an open-ended text box. Common reasons given for opting for the status quo were (a) limited income and not willing to pay any more taxes or higher prices, (b) respondent did not feel personally at risk for TFA, (c) victims should take responsibility by being more careful to avoid victimization, (d) the overall risk level for these crimes seemed small, and (e) perpetrators should pay through fines or other means.

Although there was not much variation across crime types, there was variation across the bid levels. Thus, for example, between 25% and 31% of respondents were willing to spend $250 or more, and similar but somewhat smaller numbers were willing to pay at least $500 annually. Averaging the maximum amount that each respondent was willing to pay for any crime reduction yields an estimated minimum WTP of $71.78 for IBSA, $73.16 for doxing, and $78.81 for stalking. However, as shown, the 95% confidence intervals of these three estimates overlap. This fact, coupled with the observation that each crime has substantially different incidence and harms, suggests that given the limited information provided to survey respondents, they did not confidently distinguish between the three crimes.

Table 41. Estimated Willingness-to-Pay for TFA Reduction Programs

	% > 0 (all respondents)	% > 0 if min = $250	% > 0 if min = $500	Estimated Minimum WTP	95% CI
IBSA	38.1%	30.1%	30.8%	$75.38	$67.67-$83.08
Doxing	38.1%	26.9%	26.4%	$76.95	$69.25-$84.65
Cyberstalking	40.8%	31.6%	28.1%	$82.55	$74.85-$90.24

Note that if we were to take the estimated minimum WTP at face value, we can derive a minimum amount that the average survey respondent would be willing to pay to reduce each crime. Based on the crime reduction options and bids provided by survey respondents, these figures are shown in Table 40 for the crime of stalking. Respondents were told that a 50% reduction would result in 1,600 fewer stalking incidents per 100,000 in the population. 14.66% of survey respondents chose this option with a mean bid level of $356.04, while 25.35% chose the smaller 25% reduction with a mean bid level of $106.17. Multiplying these figures and dividing by 1,600 or 800 respectively, we can add up the total willingness to pay per household for a 1 in 100,000 crime reduction—$0.06923 as shown in Table 42. This figure can be multiplied by the number of households in the U.S. to arrive at an aggregate willingness-to-pay for a 1 in 100,000 reduction in stalking of $9,097,465. Since there are 257.9 million adults over the age of 18, this would prevent 2,579 cyberstalking incidents—worth a minimum of $3,527

---

[11] Note: Approximately 5.5% of survey respondents did not answer one or more of these questions. For purposes of these tables, we have ignored those respondents and only reported on the values for those who did respond.

each ($9,097,465 / 2579). Similar calculations lead to estimates of $4,311 for IBSA and $6,535 for doxing.

While these figures are illustrative, due to the similar victim harm descriptions and the fact that there were no statistically significant differences in the minimum willingness-to-pay for 50% or 25% reductions in the three crimes, the estimated willingness-to-pay per crime shown here could be an artifact of the different crime prevalence. In other words, because stalking was the most prevalent crime, a 50% reduction results in more crimes reduced and hence a lower valuation. Overall, while we are not confident in the willingness-to-pay estimates generated by this survey, it is worth noting that the implied willingness-to-pay of $3,500 to $6,500 is less than the out-of-pocket costs to victims shown in Table 37.

Table 42. Estimated Willingness-to-Pay for Cyberstalking

Crime Reduction	Percent of Survey Responses (A)	Mean bid level (B)	(C) = A* B	Crimes reduced per 100,000 (D)	$ per household for 1 crime reduction per 100,000 population (E) = C/D
50%	.1466	$356.04	$52.20	1,600	.03262
25%	.2535	$106.17	$29.29	800	.03661
Status quo	.5999	$0	$0	0	
Total WTP per Household to reduce 1/100,000 (F)					.06923
Number of Households (G)					131,400,000
Total $ WTP (H) = F * G					$9,097,465
# of adults age 18+ / 100,000 (I)					2579
Value per victimization reduction (J) = H / I					$3,527

Regression Analysis

Aside from the dollar estimates that might be used in a benefit-cost analysis, much can be learned from further analysis of who is willing to pay more and why. To explore this further, we estimated several regression models to explain willingness-to-pay. In the first set of regressions, the dependent variable was a 0-1 dummy variable indicating whether the survey respondent was willing to pay for anything other than the status quo. The key explanatory variables of interest include the minimum dollar value shown to the respondent, their household income, demographic information, as well as a series of variables to identify their political leanings and beliefs. In addition, to proxy respondent's individual perceived risk, we included a dummy variable indicating whether they expressed concern about providing private information over the internet and whether they are regular users of social media, as well as whether they had actually reported to have been victimized by one of the TFA crimes personally in the past.

106

As shown in Table 43, survey respondents generally displayed rational economic behavior by being less willing to pay when the minimum dollar value is higher and are willing to pay more when their household income is higher.

There is also evidence that individuals who are personally more at risk are willing to pay more. In particular, respondents age 60+ were significantly less likely to be willing to pay for TFC programs, and they are much less likely to be victims themselves. On the other hand, females are more likely to pay for all three crime types—and as we saw from Tables 14 and 15, females are more likely than males to be victims of each of the three TFA crimes. Hispanic survey respondents were also more likely to pay for doxing and IBSA and are similarly more likely to be victims of these crimes. Although Blacks are also more likely than Whites to be victims, they were no more likely to pay for crime reduction programs.

Surprisingly, prior victims do not appear to be more willing to pay than non-victims. There are several possible explanations. For example, it is possible that victimization is a proxy for females who do have a somewhat higher victimization rate than males. However, the correlation is not very strong and eliminating the gender specification does not increase the significance of the victimization variable.

Another possible explanation for why victims are not more willing to pay is that the typical victim incurs no financial harms. Recall from Table 38 that even though the average victim incurred $9,515 in financial harms, only 40% of victims reported any financial harm at all. Although not shown here, replacing the "victim" variable in each of the three regressions with a dummy variable identifying victims who experienced any positive financial harms does not increase the explanatory power of the model—and none of these alternative variables are significant. Finally, it is possible that prior victims have taken their own significant precautionary measures to avoid future victimization and thus feel less personally at risk – or believe that others should take their own similar precautions instead of relying upon the government or private firms to bear a significant burden.

Among the background variables provided by IPSOS were two that were directly related to individual risk. First, respondents were asked, "How concerned are you about providing personal information over the internet?" We created a dummy variable for respondents who indicated they were "somewhat" or "very" concerned—although this variable was not significant for any of the regression models.[12] Another question asked, "Do you regularly check or post on social media on a smartphone, tablet, or other mobile device?" This variable was a statistically significant and positive explanatory variable for stalking and IBSA and was significant at p<.068 for doxing.

Finally, as expected, respondents who indicated that they think taxes are too high or that they are social conservatives were much less likely to be willing to pay for TFA reduction programs.

---

[12] Alternative specifications such as only including those "very concerned" did not provide any significant findings.

Table 43. Probit Regressions – Willingness to Pay

	IBSA		Doxing		Cyberstalking	
	Coef. (Std. Error)	p	Coef. (Std. Error)	p	Coef. (Std. Error)	p
Victim (1=Yes)	.083 (.081)	.308	.041 (.082)	.618	.037 (.081)	.652
DCE Higher Value	.000 (.000)	.881	-.001 (.000)	.165	-.000 (.000)	.561
DCE Lower Value	**-.001 (.000)**	**.005**	**-.001 (.000)**	**.001**	**-.001 (.000)**	**.001**
Sex (1=Female)	**.160 (.057)**	**.005**	**.210 (.058)**	**.000**	**.220 (.057)**	**.000**
Black (1=Yes)	-.057 (.096)	.552	.071 (.096)	.460	.036 (.095)	.707
Hispanic (1=Yes)	**.255 (.082)**	**.002**	**.310 (.083)**	**.000**	.087 (.082)	.288
Household Income	**.001 (.000)**	**.030**	**.001 (.000)**	**.003**	**.001 (.000)**	**.022**
Age Category[a]						
30-44	.035 (.091)	.702	-.037 (.091)	.684	-.007 (.089)	.936
45-59	-.122 (.092)	.184	-.072 (.093)	.436	-.118 (.090)	.191
60+	**-.213 (.090)**	**.018**	**-.203 (.090)**	**.025**	**-.245 (.088)**	**.005**
Concerned Sharing Personal Info on Social Media	.049 (.062)	.433	.087 (.063)	.168	.049 (.062)	.429
Regularly Check/Post Social Media	**.159 (.061)**	**.009**	.111 (.061)	.068	**.156 (.060)**	**.010**
Believe Taxes Are Too High	**-.559 (.059)**	**.000**	**-.575 (.060)**	**.000**	**-.587 (.059)**	**.000**
Social Conservative	**-.362 (.063)**	**.000**	**-.329 (.063)**	**.000**	**-.387 (.062)**	**.000**
Suburban Residence	.042 (.056)	.459	-.001 (.057)	.980	**-.119 (.056)**	**.034**
Constant	-.075 (.119)	.526	-.041 (.117)	.729	.173 (.118)	.145

[a] Reference category is 18-29.

Who Should Pay for TFA Crime Reduction Programs?

When responding to the DCE/willingness-to-pay questions, survey respondents were first told to ignore the question of who would pay for any new programs to reduce TFA. Specifically, they were told, "Ignore who pays for these programs directly. Instead, think about the amount the

average household should actually pay for the program—regardless of whether this is through taxes, consumer prices, or lower shareholder profits." After responding to all three DCE scenarios, they were asked, "Who do you believe should pay for programs to prevent image-based sexual abuse, doxing, and cyberstalking? (1) Government – paid for by taxes, (2) Tech companies – paid for by customers or shareholders of tech companies, or (3) Other." For those who responded "Other," a text box asked them to "please describe."

Table 44 reports on the survey responses for this question. Over all respondents, 54.6% indicated that tech companies should pay for these programs, while 27.5% indicated that taxpayers should pay. Interestingly, respondents who agreed to pay for at least one of these programs were more likely to say that tech companies should pay (58.1%). Presumably, these respondents are willing to pay through higher prices (or lower tech company profits). Similar results are shown when the sample is restricted to victims. Approximately 18% of respondents did not identify either government or tech companies as the appropriate body to pay for these programs. The reasons given varied considerably with many indicating "both," or the "perpetuators/criminals." Further analysis of these verbatim questions might prove fruitful in the future.

Table 44. Who Should Pay for Programs to Prevent TFA?

	All Respondents	Respondents who were willing to pay > 0 for at least one crime	Victims	Victims who were willing to pay > 0 for at least one crime
Government – paid for by taxes	27.5%	29.0%	30.9%	30.1%
Tech Companies – paid for by customers or shareholders of tech companies	54.6%	58.1%	51.9%	57.6%
Other	17.9%	12.9%	17.2%	12.3%

Allocation of Funds

A final question was asked of each respondent that allowed them to allocate a fixed budget among various crime control programs—or to return money to taxpayers. Specifically, the question was:

Suppose the federal government gave your mayor $1,000 per household to spend on options to reduce image-based sexual abuse, doxing, and cyberstalking in your community. Out of $1,000, how much would you spend on each program below? You can spend all of it on one program or split it up in any way you want, but the total should add up to $1,000. *(Programs randomized:)*

1. Prevention programs to educate people that these behaviors are crimes
2. Education on how to protect oneself from these crimes
3. Tougher punishment for people who commit the crimes

        4. More secure technology to prevent or reduce the harm from these crimes
        5. Victim assistance programs that provide compensation, therapy, and other services
        6. More law enforcement resources to reduce street crime such as burglary and robbery
        7. Rebate to residents

These questions were similar to those posed in previous studies on the willingness-to-pay for crime reduction programs and are patterned after well-known methodologies in the public administration literatures.[13]

        Table 45 presents the findings from this allocation experiment. The first two columns are based on the full sample, with the last two columns restricting the sample to victims. Overall, the most favored allocation is for tougher punishment, with about 21% being allocated both by victims and the public at large.

Table 45. Allocation of $1,000 per Resident

	All respondents	95% CI	Victims	95% CI
Prevention/education programs about behavior	8.7%	8.2 – 9.3%	9.9%	8.4 – 11.5%
Education to protect oneself	12.1%	11.4 – 12.7%	11.6%	9.8 – 13.4%
Tougher punishment	21.3%	20.3 – 22.2%	20.9%	18.6 – 23.2%
More secure technology	17.4%	16.6 – 18.3%	16.6%	14.7 – 18.6%
Victim assistance	14.6%	13.8 – 15.4%	17.0%	14.8 – 19.1%
More law enforcement focus on street crime	15.0%	14.2 – 15.8%	14.5%	12.5 – 16.6%
Rebate to residents	10.8%	9.8 – 11.8%	9.4%	7.1 – 11.7%

        The second highest allocation for the public at large was more secure technology (17.4%), followed by victim assistance (14.6%). In contrast, victims allocated the second most amount to victim assistance (17.0%), with more secure technology being third (16.6%)— although the confidence intervals on these two choices overlap considerably. Both victims and all respondents gave their next (fourth) priority to street crime (such as burglary and robbery) — 14.5% and 15.0% respectively. Less valued were education/prevention programs. Both victims and all respondents allocated more to educating potential victims (11.6% and 12.1%) than to programs educating potential offenders (9.9% and 8.7%). Finally, only about 10% of funds were allocated to rebates to local residents. To some extent, this low allocation to a tax rebate reflects the perceived seriousness and efficacy of more government spending on TFC offenses. However,

---

[13] See Mark A. Cohen (2015). Willingness to Pay to Reduce White-Collar and Corporate Crime. *Journal of Benefit-Cost Analysis*, 6, 305-324; as well as citations therein.

previous studies on the public's allocation of funds to crime control programs have found similar if not somewhat higher allocations to tax rebates.[14]

---

[14] For example, Cohen (2015), Table 3 reports on 11.9 – 16.3% being allocated to rebates – amounts that exceed the allocation to longer prison sentences and to law enforcement funds to reduce white collar and corporate crime.

Discussion and Conclusion

This project was guided by three research questions. In this section, we summarize the study results as they pertain to each question. The next sections discuss the study's implications for research, practice, and policy. We then conclude with a discussion of the study's limitations.

Summary of Findings

Research Question 1 asked: What are the prevalence and incidence rates associated with cyberstalking, IBSA, and doxing in the U.S.? The results of our nationally representative survey presented above revealed that approximately 16% of the respondents had experienced at least one type of TFA in their lifetime. IBSA (7.7%) was the most common individual type of lifetime TFA victimization, followed by cyberstalking (7.4%) and doxing (5.4%). Furthermore, almost 4% of respondents indicated that they had been the victim of at least two separate types of TFA. As expected, the 1-year incidence rates of TFA victimization were considerably smaller than the lifetime prevalence rates, but the victimization patterns between the two were similar. Cyberstalking (1.8%) and doxing (1.8%) were the most common individual TFA measures, followed by IBSA (1.1%). Approximately 4% of respondents reported experiencing any type of victimization in the past year, while 1.6% reported experiencing at least two types of TFA. Next, although this study primarily focused on TFA within the context of intimate partner violence (IPV), approximately 60% of IBSA and cyberstalking victims—and over 80% of doxing victims—reported that the perpetrator was someone other than a current or former intimate partner.

As discussed in the literature review, it is difficult to compare prevalence and incidence rates across studies due to differences in variable definitions, sampling frame, and time periods. In fact, as shown in Table 1, we are aware of only two previous nationally representative surveys estimating TFA offenses in the U.S.: ADL (2022) and Pew Research Center (Duggan, 2017). Our estimate of 16% lifetime prevalence of TFA is similar to the Duggan (2017) lifetime prevalence of 18% for "severe behaviors" including of physical threats, sustained harassment, stalking, and sexual harassments – a definition that might not include doxing depending upon how the survey respondent views such incidents. The ADL (2022) estimated 27% of adults had ever experienced any form of "severe" online harassment – with definitions only slightly more inclusive than our TFA categories (e.g., including swatting which was not included in our survey). In addition to the broad category of TFA, we are aware of only two nationally representative lifetime prevalence estimates for any of our three subcategories – both from the ADL (2022) survey. They found a 10% lifetime prevalence for cyberstalking and 5% for doxing, quite similar to our estimated rates of 7.4% for cyberstalking and 5.4% for doxing.

When examining the 1-year incidence rates, there were several noteworthy findings regarding the demographic profiles of TFA victims. First, women were significantly more likely to experience each of the five TFA measures compared to males, and non-cisgender respondents were more likely to experience each measure relative to both cisgender males and females. Next, White respondents were the least likely to be victimized across four of the five TFA measures (all but cyberstalking). Conversely, multiracial or 'other' race respondents were most likely to

experience each TFA measure. Regarding sexual orientation, straight respondents were less likely to experience cyberstalking, doxing, and any victimization relative to those who identify as gay/lesbian, bisexual, or another orientation. Gay/lesbian respondents were least likely to experience IBSA, while bisexual respondents were least likely to experience polyvictimization.

The average age for those who experienced TFA victimization in the past year was relatively high: 47 years old for doxing, 46 for cyberstalking, and 39 for IBSA. Next, separated respondents were most likely to experience each of the TFA measures compared to those who were married, widowed, divorced, or never married. This finding was somewhat expected for IBSA and cyberstalking since current or former intimate partners were two of the most common victim-offender relationships found in the data. Conversely, married respondents had the lowest rates of victimization in the past year for cyberstalking, doxing, and any victimization, while widowed respondents were least likely to experience IBSA.

There were few differences in past-year victimization prevalence rates regarding respondents' education level, region of residence, and employment status, and those differences that were present were quite small. The final demographic variable included in the analyses was household income. In general, respondents from lower income households were more likely to experience each TFA measure compared to those from higher income households, though this relationship was not perfectly linear. As discussed above, the patterns presented here for the 1-year incidence rates were quite similar to those of the lifetime prevalence rates (see Table 16).

This leads to Research Question 2, which was: Within the context of IPV, what are the consequences and financial costs to victims associated with cyberstalking, IBSA, and doxing? As reported by our sample of 403 self-reported victims, the potential consequences are far-reaching and vary considerably by respondent and across victimization types. Combined, the direct financial impact of victimization is estimated to be $8,874 (95% CI $4,849-$12,902), although the maximum reported in our sample was approximately $650,000. Polyvictimization had the largest mean cost of $24,848 (95% CI $8,986 - $40,731), with the largest cost borne by one of the polyvictims in our sample.

The largest component of financial costs was earnings losses – including losses due to short-term time off work as well as extended periods of time – and in some cases, shifting careers to a lower paying job. Costs associated with actual physical property were the next largest category – including stolen or vandalized property, moving expenses, and the cost associated with replacing or buying new accounts or new technology. The smallest direct financial cost categories are the out-of-pocket costs for medical or mental health expenses. However, medical and mental health expenses will inevitably be higher as nearly 40% of victims reported they were still receiving (or expected to receive) treatment in the future. Moreover, approximately 50% of victims receiving treatment reported that other sources (e.g., insurance, government programs, or nonprofits) were covering some or all of their costs – thus they are excluded from the direct financial costs to victims estimated here.

Some cost categories that make up only a small fraction of overall averages still have significant impacts on the few victims who do incur such costs. For most of the cost categories in our survey, roughly 80-90% of victims suffered no financial costs at all. For example, while the

average out-of-pocket costs for mental health care was reportedly $567, it was $5,313 for the 10.7% of victims who actually incurred these costs. Overall, 40% of victims had financial costs > 0.

In addition to monetary costs to victims, our survey also found significant identifiable non-pecuniary harms that might ultimately result in either monetary losses and/or mental anguish. For example, 64.5% of victims who were in school at the time reported having a hard time focusing on their studies while only 37.1% reported actually missing days at school. Similarly, while 37.6% of victims who were employed at the time reported difficulty focusing on their jobs, only 11.6% reported taking paid time off and 13.6% reported unpaid time off.

Similarly, while 10.7% of victims reported incurring some mental health expenses, 40% of victims reported a diagnosis of anxiety, depression, mood disorder, or PTSD compared to about 20% for non-victims. Thus, not only do victims have a higher rate of mental health issues, the need for mental health care for victims appears to be much higher than the rate of victims receiving such care. These findings alone do not necessarily establish causality – as it is possible that those afflicted with one of these mental health disorders are more vulnerable to IPV victimization. This is an area where further study could prove fruitful.

In addition to variability in victimization rates by demographic characteristics, we also found two statistically significant differences in financial impacts. First, victims in the 30-59 age range had higher losses than those under 30 or 60+. This is most likely due to the fact that these victims are more likely to be working at the time of victimization. Indeed, the total financial impact for victims who were working is about twice that of the non-working, and the average age of employed victims was about 40 compared to 55 for non-employed victims. Second, the financial costs actually decrease with household income. Thus, controlling for the rate of victimization, the financial impact of TFAs have a disproportionate impact on lower income individuals.

Finally, one of our research questions was to understand the differing impact on minors who were victims of TFA. Although the sample was limited to adults over age 18, we were able to estimate the number of minors by comparing their current age to the date of their most recent victimization. Overall, only 13.1% of our victim sample were estimated to have been victimized as minors – resulting in a sample of only 53 victims. Nevertheless, based on that limited sample, the direct monetary costs to minors is estimated to be about 1/3 that of non-minors. Of course, these are not directly comparable since adults who were victimized many years ago as minors are included in our "non-minor" sample, and even for those who we were able to include in our "minors" subcategory might incur ongoing financial costs.

Finally, Research Question 3 asked: What is the public's willingness-to-pay to reduce the risk and consequences of cyberstalking, IBSA, and doxing in the U.S.? To address this question, we posed a series of hypotheticals to survey respondents designed to elicit this information. On average, we found that the typical individual was willing to pay between $75 and $85 annually to reduce each of the three crime types. However, when averaged over the entire population, These figures translate into an estimated willingness-to-pay to reduce one TFA incident ranges from about $3,500 to $6,500.

Our first major finding was that the implied willingness-to-pay to reduce one victimization is less than the estimated financial burden to victims that was estimated in the portion of the survey that victims responded to. Although the reason for this is unclear, it is possible that respondents underestimated the true costs and consequences of victimization. This might have been exacerbated by the brief descriptions given of each TFA that did not include quantifiable impacts. However, based on open-ended survey responses explaining their choice on the survey, several other possibilities became clear. First, some respondents noted that the underlying rates of victimization were low and thus spending money on further reducing their incidence would not be their priority. Second, some survey respondents shifted some or all of the blame on victims – who they said should have taken more precautions. No doubt a combination of all three reasons contributed to this finding.

Further analysis of respondent's willingness-to-pay revealed several interesting findings. First, women and Hispanics were generally willing to pay more than men and non-Hispanics, as were those who reported they regularly check and/or post social media. These three groups are also those who are at higher risk for victimization. Those aged 60+ were found to be willing to pay less – which is also consistent with their lower risk of victimization. Prior victims were not willing to pay any more than non-victims, controlling for other demographics. One possible reason for this finding is that the typical victim suffers no financial costs (i.e., only 40% of victims reported costs greater than zero). Alternatively, prior victims might have taken further precautions and believe they are now at lower risk, and/or these precautions should be taken by a larger percentage of the population.

Additional insights from the willingness-to-pay survey came from follow-up questions. First, approximately 55% of respondents believe that tech companies should pay for programs to reduce TFA (whether through lower corporate profits or higher consumer prices), while 27.5% believe the burden should be on taxpayers. The remaining 18% indicated various parties should pay – such as a combination of taxpayers and companies, perpetrators (through higher fines), and victims themselves (although this was a small minority of respondents).

Finally, when asked to rank the relative importance of taxpayer spending to address TFA, the highest ranked was tougher punishment, followed by victim assistance and more secure technology. Educational programs to either prevent such abusive behavior or to protect oneself from becoming a victim were given lower priority.

Implications for Research

This study has several implications for future research, practices, and policy regarding technology-facilitated abuse. The implications and recommendations presented in the following sections are based primarily on our survey findings but are complemented by input from our project partners, interviews with SMEs, and project advisory board meetings.

The current findings indicate that non-cisgender respondents experience higher rates of IBSA, cyberstalking, any victimization, and polyvictimization compared to cisgender individuals. However, the small baseline numbers of non-cisgender respondents in this survey

(n=38) points to a need for further analysis. Researchers should consider oversampling non-cisgender individuals in future studies to ensure a more robust analysis of their victimization rates.

Next, it is important to highlight our findings regarding the substantial economic burden on TFA victims, including property damage, moving costs, high mental and physical health costs, expenses for new technology, lost tuition, and unpaid earnings. These results could be used in future cost-benefit analyses with the understanding that they only represent tangible costs to victims – and exclude tangible costs to the government and private sector, as well as intangible victim and non-victim costs.[15] To our knowledge, this is novel information, as it has not been rigorously studied in the U.S. before, at least in the context of IBSA. Future research might expand upon this study by attempting to estimate the costs of TFA to government and private sectors. In addition, refining and expanding upon the willingness-to-pay portion of our survey might lead to more robust intangible cost estimates.

As discussed above, there is little to no consistency in past studies' definitions of TFA in general, as well as the three types of TFA included in this study. This lack of consistency has a significant impact on comparing findings across studies. The combination of our extensive literature review, interviews with SMEs, and advisory board meetings offers more robust definitions of TFA and its subcomponents that can be used in future research. These activities also led to an expanded and more comprehensive taxonomy of the harms and costs of TFA victimization.

Finally, the data from this study reveal the nuances of three types of technology-facilitated abuse: IBSA, cyberstalking, and doxing. Including this study, there is now a relatively large body of research on TFA. It is recommended that future research incorporate these findings—as well as our definitions and taxonomy of harms—and begin focusing on the remaining gaps in knowledge to gain a deeper understanding of these specific forms of TFA. This will allow researchers to then partner with advocates and practitioners to implement the recommendations borne from the research.

Implications for Practice

As shown in the results above (e.g., see Table 14), members of certain demographic groups are significantly more likely to experience TFA victimization relative to others. As such, victim service providers and policymakers may need to assess how their resources are being deployed across demographics to ensure that those in most need are adequately served.

The current findings indicate that straight respondents are less likely to be victims of IBSA, cyberstalking, any victimization, and polyvictimization compared to those who identify as gay/lesbian, bisexual, or another orientation. Furthermore, the higher victimization rates among

---

[15] The SMEs in our study argued that researchers, policy makers, NGOs, and civil society should encourage tech companies to take responsibility for covering these costs rather than leaving victims and survivors to bear them alone.

bisexual and 'other' respondents compared to gay/lesbian individuals suggest the need for nuanced interventions. Based on these results, stakeholders—including policymakers, funders, service providers, and community organizations—should collaborate to create inclusive, culturally competent support systems that are accessible and responsive to the diverse needs of LGBTQI+ individuals.

Our results lead to a number of recommendations for victim-service providers and law enforcement. First, TFA has impacts that are not just online and that are tied to other kinds of abuse. As such, service providers and law enforcement should ask about both tangible and intangible costs when supporting survivors. Second, advocates should work to strengthen partnerships with other service providers who can assist with the tangible costs experienced by TFA victims. Similarly, victim service providers should support survivors in dealing with intangible harms, and refer them to partners (e.g., mental health) when needed. Finally, service providers and advocates might consider additional measures to help survivors develop safety plans and privacy strategies for costs related to reputational damage, technology, employment, housing, and other impacts from TFA victimization.

As shown above, TFA victimization can also impact students' success and well-being. Our survey results, combined with input from the SMEs, led us to several education-related recommendations. First, educational administrators should train faculty/teachers and staff on how to (1) recognize potential signs of abuse; (2) reach out to potential victims of TFA; and (3) design online learning environments to support student safety and privacy. Next, campus and school violence intervention and prevention programs should ensure they address TFA as these offenses are common among young adults. Similarly, administrators should review their existing policies and practices to account for TFA in anti-harassment and abuse efforts. Finally, as TFA is becoming more common, institutions of higher education should support faculty and student-led research on TFA issues.

It is also important to note that care should be taken to avoid any implication of victim blaming while interpreting or disseminating these research findings. For example, 69% of survey respondents expressed significant concern about sharing personal information online; however, it is important to focus on systems-level solutions to TFA rather than on an individuals' information or image-sharing practices.

Implications for Policy

This research primarily focused on TFA within the context of intimate partner violence (IPV). Though approximately 40% of both IBSA and cyberstalking victims indicated the perpetrator was a current or former intimate partner, survey results revealed that nearly 60% of cases involved non-intimate or unknown individuals. Policymakers and tech companies should therefore address TFA cases both inside and outside of intimate partner relationships, ensuring comprehensive strategies for all victims and survivors. In addition, where lacking, policies and programs should be instituted to support survivors with housing, employment, financial technology security, and education impacts (e.g., breaking leases, employment leave related to abuse, identity and fraud protection)

Based on our results, it is particularly important to emphasize the impacts of TFA for lower-income and other marginalized communities when shaping policy response. Challenges in accessing technology can impact personal safety and well-being, and disproportionately affects many of the same communities indicated in this study as being more likely to experience TFA victimization. Therefore, programs to increase access to broadband, internet access, devices, and phone lines will assist survivors. Furthermore, given the significant costs associated with TFA, policymakers and funders should ensure that support services are affordable for all income levels. Special attention should be given to those with incomes under $10,000, including providing more robust financial assistance programs to help manage TFA-related costs.

Limitations

As with any research, this study had limitations. First, approximately 40% of TFA victims reported a diagnosis of anxiety, depression, mood disorder, or PTSD compared to about 20% for non-victims. However, these are simple correlations; we cannot infer any causality here because we do not know whether a mental health diagnosis came before or after respondents' TFA victimization. Further research could employ a more longitudinal approach to studying TFA victimization to determine whether there are specific causal mechanisms that explain the relationship between TFA victimization and mental health diagnoses.

Next, because about 25% of TFA victims in our study were polyvictims—whose total costs related to victimization were much higher than any one of the three individual TFA measures included in this study—any reference to financial costs of one offense type might significantly underestimate costs. An alternative estimate that combines all three offenses might be a more defensible approach. This is why the harms and costs tables in our study include an "All Victims" category. Furthermore, our estimates of the monetary costs of TFA victimization are likely conservative and limited by the long-term nature of many of the harms and costs. For example, we were unable to capture many of the long-term costs to victims who suffer ongoing mental health issues or changes in career trajectories. Future studies incorporating a longitudinal research design would help address this limitation as well.

Finally, our survey did not include an explicit question asking how old respondents were when they experienced TFA victimization. As discussed on page 81, we were able to estimate whether victims were under 18 years old at the time of their victimization, but this estimate is likely very conservative. Future research should more specifically delineate between whether victimization experiences occurred as an adult or a minor. Given the significant differences in laws that protect minors and those that protect adults, this distinction can provide important information for service providers, law enforcement, and policymakers.

References

Abu-Ulbeh, W., Altalhi, M., Abualigah, L., Almazroi, A. A., Sumari, P., & Gandomi, A. H. (2021). Cyberstalking victimization model using criminological theory: A systematic literature review, taxonomies, applications, tools, and validations. *Electronics*, *10*(14), 1670.

Afrouz, R. (2021). The nature, patterns and consequences of technology-facilitated domestic abuse: A scoping review. *Trauma, Violence & Abuse*, 152483802110467. Advanced online publication, https://doi.org/10.1177/15248380211046752.

Agnew, R. (1992). Foundation for a general strain theory of crime and delinquency. *Criminology, 30*(1), 47-88.

Ahlgrim, B., & Terrance, C. (2021). Perceptions of cyberstalking: Impact of perpetrator gender and cyberstalker/victim relationship. Journal of interpersonal violence, 36(7-8), NP4074-NP4093.

Akers, R.L., Sellers, C., & Jennings. (2016). *Criminological theories: Introduction, evaluation, and application (7th edition)*. Cambridge: Oxford University Press.

Alahmad, Y. Y., & Bata, H. (2021). Cyber Workplace Bullying: An Empirical Study. *American Journal of Industrial and Business Management*, *11*(7), 767-784.

Almond, L., McManus, M. A., & Chatterton, H. (2020). Internet facilitated rape: A multivariate model of offense behavior. *Journal of interpersonal violence, 35*(21-22), 4979-5004.

Al-Rahmi, W. M., Yahaya, N., Alamri, M. M., Aljarboa, N. A., Kamin, Y. B., & Saud, M. S. B. (2019). How cyber stalking and cyber bullying affect students' open learning. *Ieee Access*, *7*, 20199-20210.

Anderson, B., & Wood, M. A. (2021). Doxing: A Scoping Review and Typology. The Emerald International Handbook of Technology Facilitated Violence and Abuse, Emerald Publishing Limited, 205-226.

Anderson, D.A. (2011). The Cost of Crime. Foundations and Trends in Microeconomics: 7, 209–265.

Andrighetto, L., Riva, P., & Gabbiadini, A. (2019). Lonely hearts and angry minds: Online dating rejection increases male (but not female) hostility. *Aggressive behavior*, *45*(5), 571-581.

Anti-Defamation League. (2022). *Online hate and harassment: The American experience*. Retrieved from: https://www.adl.org/resources/report/online-hate-and-harassment-american-experience-2022.

Anwar, A., Kee, D. M. H., & Ahmed, A. (2020). Workplace cyberbullying and interpersonal deviance: understanding the mediating effect of silence and emotional exhaustion. *Cyberpsychology, Behavior, and Social Networking*, *23*(5), 290-296.

Arrow, K., Solow, R., Portney, P., Leamer, E., Radner, R. & Schuman, H. (1993). *Report of the NOAA Panel on Contingent Valuation*. Washington, DC: National Oceanic and Atmospheric Administration

Bailey, J., & Mathen, C. (2017). *Technologically-facilitated violence against women and girls: If criminal law can respond, should it?* Ottawa Faculty of Law Working Paper, (2017-44).

Bailey, J., & Shayan, S. (2021). The Missing and Murdered Indigenous Women Crisis: Technological Dimensions. In Bailey, J., Flynn, A. and Henry, N. (Eds.), The Emerald International Handbook of Technology Facilitated Violence and Abuse. Emerald Publishing Limited.

Baker, C. K., & Carreño, P. K. (2016). Understanding the role of technology in adolescent dating and dating violence. *Journal of child and family studies*, *25*(1), 308-320.

Barter, C., & Stanley, N. (2016). Inter-personal violence and abuse in adolescent intimate relationships: mental health impact and implications for practice. *International review of psychiatry*, *28*(5), 485-503.

Bates, S. (2017). Revenge porn and mental health: A qualitative analysis of the mental health effects of revenge porn on female survivors. *Feminist Criminology*, *12*(1), 22-42.

Bath, H. (2008). The three pillars of trauma-informed care. Reclaiming Children and Youth, 17(3), 17–21. Retrieved from: https://www.hope.ms.gov/sites/mccj/files/Hope%20training%20January%202021/read_3 %20Pill ars%20of%20TIC.pdf.

Baum, K., Catalano, S., Rand, M., & Rose, K. (2009). *Stalking victimization in the United States*. U.S. Department of Justice, Bureau of Justice Statistics.

Begotti, T., & Acquadro Maran, D. (2019). Characteristics of cyberstalking behavior, consequences, and coping strategies: A cross-sectional study in a sample of Italian university students. *Future Internet*, *11*(5), 120.

Bianchi, D., Morelli, M., Nappa, M. R., Baiocco, R., & Chirumbolo, A. (2021). A bad romance: Sexting motivations and teen dating violence. *Journal of interpersonal violence, 36*(13-14), 6029-6049.

Biderman, A. D., & Reiss Jr, A. J. (1967). On exploring the" dark figure" of crime. *The Annals of the American Academy of Political and Social Science*, *374*(1), 1-15.

Blythe, J.M., Johnson, S.D. & Manning, M. (2020). What is security worth to consumers? Investigating willingness to pay for secure Internet of Things devices. *Crime Science 9(1)*, 1-9.

Borrajo, E., Gamez-Guadix, M., & Calvete, E. (2015). Cyber dating abuse: Prevalence, context, and relationship with offline dating aggression. *Psychological Reports: Relationships & Communications*, *116*, 565-585.

Borrajo, E., Gamez-Guadix, M., Pereda, N., & Calvete, E. (2015). The development and validation of the cyber dating abuse questionnaire among young couples. *Computers in Human Behavior*, *48*, 358-365.

Braddock, K., Hughes, B., Goldberg, B., & Miller-Idriss, C. (2021). Subversive Online Activity Predicts Susceptibility to Persuasion by Far-Right Extremist Propaganda [Pre-print]. MediArXiv Preprints. Retrieved from: https://mediarxiv.org/c734s/.

Brady, K. M. (2017). Revenge in modern times: The necessity of a federal law criminalizing

revenge porn. Hastings Women's Law Journal: 28, 3.

Brem, M. J., Florimbio, A. R., Grigorian, H., Wolford-Clevenger, C., Elmquist, J., Shorey, R. C., Rothman, E. F., Temple, J. R., & Stuart, G. L. (2019). Cyber abuse among men arrested for domestic violence: Cyber monitoring moderates the relationship between alcohol problems and intimate partner violence. *Psychology of Violence*, *9*, 410-418.

Brown, M. L., Reed, L. A., & Messing, J. T. (2018). Technology-based abuse: Intimate partner violence and the use of information communication technologies. In J. Vickery & T. Everbach (Eds.) Mediating misogyny: Gender, technology, and harassment, (pp. 209-227). Palgrave Macmillan.

Bundock, K., Chan, C., & Hewitt, O. (2020). Adolescents' help-seeking behavior and intentions following adolescent dating violence: A systematic review. *Trauma, Violence, & Abuse*, *21*(2), 350-366.

Burke, S. C., Wallen, M., Vail-Smith, K., & Knox, D. (2011). Using technology to control intimate partners: An exploratory study of college undergraduates. *Computers in Human Behavior*, *27*, 1162–1167.

Carlson, B., & Frazer, R. (2021). Attending to difference in indigenous people's experiences of cyberbullying: Toward a research agenda. *The Emerald International Handbook of Technology-Facilitated Violence and Abuse*, 145-163.

Carson, R. T., & Louviere, J. J. (2017). Estimation of broad-scale tradeoffs in community policing policies. *Journal of Benefit-Cost Analysis*, *8*(3), 385-398.

Cava, M. J., Tomas, I., Buelga, S., & Carrascosa, L. (2020). Loneliness, depressive mood and cyberbullying victimization in adolescent victims of cyber dating violence. *International Journal of Environmental Research and Public Health*, *17*, 4269-4285.

Chalfin, A. (2015). Economic costs of crime. *The encyclopedia of crime and punishment*, 1-12.

Chen, Q., Chan, K. L., & Cheung, A. S. Y. (2018). Doxing victimization and emotional problems among secondary school students in Hong Kong. *International journal of environmental research and public health*, *15*(12), 2665.

Chen, M., Cheung, A. S. Y., & Chan, K. L. (2018). Doxing: What adolescents look for and their intentions. *International journal of environmental research and public health*, *16*(2), 218.

Cheyne, N., & Guggisberg, M. (2018). Stalking: An age old problem with new expressions in the digital age. In M. Guggisberg & J. Henricksen (Eds.), *Violence against women in the 21st Century: Challenges and* future directions, 161-190.

Choi, K. S. (2008). Computer crime victimization and integrated theory: An empirical assessment. *International Journal of Cyber Criminology*, *2*(1).

Citron, D. (2021). A New Compact for Sexual Privacy, 62 Wm. & Mary L. Rev. 1763 https://scholarship.law.wm.edu/wmlr/vol62/iss6/2

Citron, D. K., & Franks, M. A. (2014). Criminalizing revenge porn. *Wake Forest L. Rev.*, *49*, 345.

Clear, T.R., & Austin, J.F. (2021). Rehabilitation for "cost of crime" models. *Journal of Policy*

Analysis and Management, 40(1), 294-300.

Clevenger, S., & Gilliam, M. (2020). Intimate Partner Violence and the Internet: Perspectives. *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, 1333-1351.

Clevenger, S., & Navarro, J. (2021). The "third-victimization": The cybervictimization of sexual assault survivors and their families. *Journal of Contemporary Criminal Justice*, *37*(3), 356-378.

Clevenger, S. L., Navarro, J. N., & Gilliam, M. (2018). Technology and the endless "cat and mouse" game: A review of the interpersonal cybervictimization literature. *Sociology Compass*, *12*, e12639-e12651.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, *44*, 588-608.

Cohen, L. E., Kluegel, J. R., & Land, K. C. (1981). Social inequality and predatory criminal victimization: An exposition and test of a formal theory. *American sociological review*, 505-524.

Cohen, M.A., & Farrington, D.P. (2021). Appropriate measurement and use of "costs of crime" in policy. *Journal of Policy Analysis and Management, 40*(1), 284-293.

Cohen, M. A. (2020). *The costs of crime and justice, 2ⁿᵈ Ed*. Routledge, Taylor & Francis.

Cohen, M.A., & Bowles, R. (2010). Estimating Costs of Crime. In A. Piquero & D. Weisburd (Eds.), *Handbook of Quantitative Criminology*, *1ˢᵗ Ed.,* 143-162. New York: Springer.

Cohen, M. A. & Miller, T. R. (1998) The Cost of Mental Health Care for Victims of Crime, *Journal of Interpersonal Violence, 13(1)*, 93–110.

Cohen, M.A., Miller, T.R. & Rossman, S.B, The Costs and Consequences of Violent Behavior in the United States, in <u>*Understanding and Preventing Violence: Consequences and Control of Violence*</u>, Vol. 4, National Research Council. (Washington, D.C.: National Academy Press), 1994, pp. 67-166.

Cohen, M.A, Rust, R.T., Steen, S. & Tidd, S.T. (2001). Willingness-to-pay for crime control programs. *Criminology, 42*(1), 89-110.

Cohen, M. A., & Piquero, A. R. (2009). New evidence on the monetary value of saving a high-risk youth. *Journal of Quantitative Criminology*, *25*(1), 25-49.

Cook, P. J. (1983). Crime Statistics: Costs of Crime. In S.H. Kadish (Ed.), *Encyclopedia of Crime and Justice, Vol. 1*. New York, NY: Free Press.

Copp, J. E., Mumford, E. A., & Taylor, B. G. (2021). Online sexual harassment and cyberbullying in a nationally representative sample of teens: Prevalence, predictors, and consequences. *Journal of Adolescence*, *93*, 202-211.

Curry, T. R., & Zavala, E. (2020). A multi-theoretical perspective on cyber dating abuse victimization and perpetration within intimate relationships: A test of general strain, social learning, and self-control theories. *Victims & Offenders*, *15*(4), 499-519.

Cyber Civil Rights Initiative. (n.d.). *Frequently asked questions*.

https://cybercivilrights.org/faqs/#terminolog

Dardis, C. M., Strauss, C. V., & Gidycz, C. A. (2019). The psychological toll of unwanted pursuit behaviors and intimate partner violence on undergraduate women: A dominance analysis. *Psychology of Violence*, *9*(2), 209.

Davis, J. P., Dumas, T. M., Berey, B., Merrin, G. J., Tan, K., & Madden, D. R. (2018). Poly-victimization and trajectories of binge drinking from adolescence to young adulthood among serious juvenile offenders. *Drug and alcohol dependence*, *186*, 29-35.

Davis, J. P., Dworkin, E. R., Helton, J., Prindle, J., Patel, S., Dumas, T. M., & Miller, S. (2019). Extending poly-victimization theory: Differential effects of adolescents' experiences of victimization on substance use disorder diagnoses upon treatment entry. *Child Abuse & Neglect*, *89*, 165-177.

Debreu, G. (1964). Continuity properties of Paretian utility. *International Journal of Economics, 5*(3), 285-293.

Delker, B. C., & Freyd, J. J. (2014). From betrayal to the bottle: Investigating possible pathways from trauma to problematic substance use. *Journal of traumatic stress*, *27*(5), 576-584.

Dhillon, G., & Smith, K. J. (2019). Defining objectives for preventing cyberstalking. *Journal of Business Ethics*, *157*(1), 137-158.

Dick, R. N., McCauley, H. L., Jones, K. A., Tancredi, D. J., Goldstein, S., Blackburn, S., Monasterio, E., James, L., Silverman, J. G., & Miller, E. (2014). Cyber dating abuse among teens using school-based health centers. *Pediatrics*, *134*, e1560-e1567.

Dobash, R. E., & Dobash, R. (1979). *Violence against wives: A case against the patriarchy*. New York: Free Press.

Dominguez, P. & Raphael, S. (2015). The role of the cost-of-crime literature in bridging the gap between social science research and policy making: Potentials and limitations. *Criminology & Public Policy, 14*(4), 589-632.

Douglas, H., Harris, B. A., & Dragiewicz, M. (2019). Technology-facilitated domestic and family violence: Women's experiences. *British Journal of Criminology*, *59*, 551-570.

Dragiewicz, M. (2021). Best practice principles for measurement of technology-facilitated coercive control. In B. Harris and D. Woodlock (Eds) *The Routledge Handbook of Technology and Domestic Violence*, Routledge.

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

Dragiewicz, M., Harris, B., Woodlock, D., …, Milne, L. (2019) *Domestic violence and technology: Survivor experiences of intrusion, surveillance, and identity crime*. Sydney: Australian Communications Consumer Action Network.

Drouin, M., Ross, J., & Tobin, E. (2015). Sexting: A new, digital vehicle for intimate partner aggression?. *Computers in human behavior*, *50*, 197-204.

Duerksen, K. N., & Woodin, E. M. (2019). Technological intimate partner violence: Exploring

technology-related perpetration factors and overlap with in-person intimate partner violence. *Computers in Human Behavior, 98*, 223-231.

Duggan, M. (2014). Online Harassment 2014. Pew Research Center. Retrieved from: http://www.pewinternet.org/2014/10/22/onlineharassment/

Duggan, M. (2017). *Online harassment 2017*. Pew Research Center. Retrieved from: https://www.pewresearch.org/internet/2017/07/11/online-harassment-2017/

Dunn, S. (2020). *Technology-facilitated gender-based violence: An overview (Supporting a Safer Internet No. 1; pp. 1–30)*. Centre for International Governance and Innovation.

Eaton, A.A., Jacobs, H., & Ruvalcaba, Y. (2017). 2017 *Nationwide online study of nonconsensual porn victimization and perpetration*. Cyber Civil Rights Initiative. Retrieved from: https://www.cybercivilrights.org/wpcontent/uploads/2017/06/CCRI-2017-Research-Report.pdf

Eaton, A. A., & McGlynn, C. (2020). The psychology of nonconsensual porn: Understanding and addressing a growing form of sexual violence. *Policy Insights from the Behavioral and Brain Sciences*, *7*(2), 190-197.

Eaton, A. A., Ramjee, D., & Saunders, J. F. (2022). The Relationship between Sextortion during COVID-19 and Pre-pandemic Intimate Partner Violence: A Large Study of Victimization among Diverse US Men and Women. *Victims & Offenders*, 1-18.

Eterovic-Soric, B., Choo, K. K. R., Ashman, H., & Mubarak, S. (2017). Stalking the stalkers–detecting and deterring stalking behaviours using technology: A review. *Computers & security*, *70*, 278-289.

Fernet, M., Lapierre, A., Hébert, M., & Cousineau, M.-M. (2019). A systematic review of literature on cyber intimate partner victimization in adolescent girls and women. Computers in Human Behavior, 100, 11-25.

Finkelhor, D., Turner, H., & Colburn, D. (2022). Prevalence of online sexual offenses against children in the US. *JAMA network open*, *5*(10), e2234471-e2234471.

Finkelhor, D., Walsh, K., Jones, L., Mitchell, K., & Collier, A. (2021). Youth internet safety education: Aligning programs with the evidence base. *Trauma, violence, & abuse*, *22*(5), 1233-1247.

Fiolet, R., Brown, C., Wellington, M., Bentley, K., & Hegarty, K. (2021). Exploring the impact of technology-facilitated abuse and its relationship with domestic violence: a qualitative study on experts' perceptions. *Global qualitative nursing research*, *8*, 23333936211028176.

Fissel, E. R. (2019). *Victimization of the 21ˢᵗ century: An examination of cyberstalking victimization using a target congruence approach*. [Doctoral dissertation, University of Cincinnati]. OhioLINK. Retrieved from: http://rave.ohiolink.edu/etdc/view?acc_num=ucin1553613508435002

Fissel, E. R. (2021). The reporting and help-seeking behaviors of cyberstalking victims. *Journal of Interpersonal Violence, 36*, 11-12, 5075-5100.

Fissel, E. R., Fisher, B. S., & Wilcox, P. (2023). Do vulnerability, gratifiability, and antagonism

explain cyberstalking victimization among young adults? *Criminal Justice and Behavior*, *50*, 1380-1404.

Fissel, E. R., Reyns, B. W., Nobles, M. R., Fisher, B. S., & Fox, K. A. (2024). Cyberstalking victims' experiences with fear versus other emotional responses to repeated online pursuit: Revisiting the fear standard among a national sample of young adults. *Crime & Delinquency*, *70*, 1116-1147.

Flach, R. M. D., & Deslandes, S. F. (2017). Cyber dating abuse in affective and sexual relationships: a literature review. *Cadernos de saude publica*, *33*.

Flynn, A., Powell, A., & Hindes, S. (2021). Technology-facilitated abuse: A survey of support services stakeholders (Research report, 02/2021). ANROWS.

Flynn, A., Powell, A., & Hindes, S. (2023). Policing technology-facilitated abuse. *Policing and Society*, *33*, 575-592.

Foley, K. G. (2021). "But, I Didn't Mean to Hurt You": Why the First Amendment Does Not Require Intent-to-Harm Provisions in Criminal" Revenge Porn" Laws. *Boston College Law Rev.*, *62*, 1365.

Ford, J. D., Elhai, J. D., Connor, D. F., & Frueh, B. C. (2010). Poly-victimization and risk of posttraumatic, depressive, and substance use disorders and involvement in delinquency in a national sample of adolescents. *Journal of Adolescent Health*, *46*(6), 545-552.

Franks, M. A. (2016). *Doxing, swatting, trolls, and SJWs: Harassment and gender discrimination on social media platforms*. American Bar Association, Committee on Copyright and Social Media: Bethesda, MD.

Franks, M. A. (2017). Revenge porn reform: A view from the front lines. *Florida Law Rev.*, *69*, 1251.

Franks, M. A. (2019). *The crime of "revenge porn".* In L. Alexander and K. K. Ferzan (Eds.), The Palgrave Handbook of Applied Ethics and the Criminal Law (pp. 661-692). Springer International Publishing.

Fraser, C., Olsen, E., Lee, K., Southworth, C., & Tucker, S. (2010). The new age of stalking: Technological implications for stalking. *Juvenile and family court journal*, *61*(4), 39-55.

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

Freed, D., Palmer, J., Minchala, D., Levy, K., Ristenpart, T., & Dell, N. (2018). "A Stalker's Paradise" How Intimate Partner Abusers Exploit Technology. In *Proceedings of the 2018 CHI conference on human factors in computing systems* (pp. 1-13).

Gamez-Guadix, M., Almendros, C., Borrajo, E., & Calvete, E. (2015). Prevalence and association of sexting and online sexual victimization among Spanish adults. *Sexuality Research and Social Policy*, *12*, 145-154.

Gavin, J., & Scott, A. J. (2019). Attributions of victim responsibility in revenge pornography. *Journal of Aggression, Conflict and Peace Research, 11*(4), 263-272.

Gendera, S., & Breckenridge, J. (2021). The significance of technology as both a resource in enhancing safety, and a means of perpetrating violence: the implications for policy and practice. *Journal of gender-based violence, 5*(3), 413-429.

Higgins, G. E., & Nicholson, J. (2020). The General Theory of Crime. In *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (pp. 567-581). Palgrave Macmillan, Cham.

Gini, G., Card, N. A., & Pozzoli, T. (2018). A meta-analysis of the differential relations of traditional and cyber-victimization with internalizing problems. Aggressive Behavior, 44(2), 185-198.

Goldstein, J. (2020). Revenge porn' was already commonplace. The pandemic has made things even worse. *The Washington Post*.

Gosse, C. (2021). "Not the Real World": Exploring Experiences of Online Abuse, Digital Dualism, and Ontological Labor. In *The Emerald International Handbook of Technology-Facilitated Violence and Abuse*. Emerald Publishing Limited.

Gottfredson, M. R., & Hirschi, T. (1990). A general theory of crime. In *A General Theory of Crime*. Stanford University Press.

Government Accountability Office (2017). Cost of Crime: Experts Report Challenges Estimating Costs and Suggest Improvements to Better Inform Policy Decisions. (GAO-17-732). Government Accountability Office (GAO)Washington, DC: U.S. Government Printing Office. Retrieved from: https://www.gao.gov/products/gao-17-732.

Graham, A., Kulig, T. C., & Cullen, F. T. (2019). Willingness to report crime to the police: Traditional crime, cybercrime, and procedural justice. *Policing: An International Journal*, *43*(1), 1-16.

Grimani, A., Gavine, A., & Moncur, W. (2020). An evidence synthesis of covert online strategies regarding intimate partner violence. *Trauma, Violence, & Abuse*, 1524838020957985.

Halbesleben, J. R., Neveu, J. P., Paustian-Underdahl, S. C., & Westman, M. (2014). Getting to the "COR" understanding the role of resources in conservation of resources theory. *Journal of management*, *40*(5), 1334-1364.

Harris, B. (2018). Spacelessness, spatiality and intimate partner violence: Technology-facilitated abuse, stalking and justice administration. In K. Fitz-Gibbon, S. Walklate, J. McCulloch, and J. Maher (eds.), *Intimate partner violence, risk and security* (pp. 52-70). Routledge.

Harris, B. A., & Woodlock, D. (2019). Digital coercive control: Insights from two landmark domestic violence studies. *The British Journal of Criminology*, *59*(3), 530-550.

Hay, C., & Ray, K. (2020). General strain theory and cybercrime. *The Palgrave handbook of international cybercrime and cyberdeviance*, 583-600.

Henry, N., Vasil, S., Flynn, A., Kellard, K., & Mortreux, C. (2022). Technology-facilitated domestic violence against immigrant and refugee women: A qualitative study. *Journal of interpersonal violence*, *37*(13-14), NP12634-NP12660.

Hinduja, S., & Patchin, J. W. (2020). Digital dating abuse among a national sample of U.S.

youth. *Journal of Interpersonal Violence*, *36*, 11088-11108.

Hobfoll, S. E., Tirone, V., Holmgreen, L., & Gerhart, J. (2016). Conservation of resources theory applied to major stress. In G. Fink (Ed.), Handbook of stress Vol. 1: Concepts, cognition, emotion, and behavior (pp. 65–71). Cambridge, MA: Elsevier Academic Press.

Homchick, N. (2019). Reaching through the Ghost Doxer: An Argument for Imposing Secondary Liability on Online Intermediaries. Washington & Lee Law Review, 76, 1307.

Hunink, M, Glasziou, P., …, & Weinstein, M.C. (2001). *Decision making in health and medicine: Integrating evidence and values.* Cambridge University Press.

Johnson, M. (2008). A typology of domestic violence. Boston: Northeastern Press.

Kaur, P., Dhir, A., Tandon, A., Alzeiby, E. A., & Abohassan, A. A. (2021). A systematic literature review on cyberstalking. An analysis of past achievements and future promises. *Technological Forecasting and Social Change*, *163*, 120426.

Kling, C. L., Phaneuf, D. J., & Zhao, J. (2012). From Exxon to BP: Has some number become better than no number?. *Journal of Economic Perspectives*, *26*(4), 3-26.

Kowert, R., & Cook, C. (2022, January). The toxicity of our (virtual) cities: Prevalence of dark participation in games and perceived effectiveness of reporting tools. In *Proceedings of the 55th Hawaii International Conference on System Sciences*.

Kraft, E., & Wang, J. (2010). An exploratory study of the cyberbullying and cyberstalking experiences and factors related to victimization of students at a public liberal arts college. *International Journal of Technoethics*, *1*, 74-91.

Lageson, S. E., McElrath, S., & Palmer, K. E. (2019). Gendered public support for criminalizing "Revenge Porn". *Feminist criminology*, *14*(5), 560-583.

Lee, K., & Anderson, J. (2016). The internet and intimate partner violence: Technology changes, abuse doesn't. *Criminal Justice, 31*, 28-33.

Lee, J.G. & Fisher, D. (2020). The influence of scope, frames, and extreme willingness to pay responses on cost of crime estimates. *American Journal of Criminal Justice, 45,* 236-272.

Lenhart, A., Michelle, Y., & Price-Feeney, M. (2016). Nonconsensual image sharing: One in 25 Americans has been victim of "revenge porn." Data & Society Research Institute and Centre for Innovative Public Health Research data memo. Retrieved from https://datasociety.net/pubs/oh /Nonconsensual_Image_Sharing_2016.pdf

Lenhart, A., Ybarra, M., Zickuhr, K., & Price-Feeney, M. (2016b). *Online harassment, digital abuse, and cyberstalking in America*. Data and Society Research Institute.

Levy, K., & Schneier, B. (2020). Privacy threats in intimate relationships. *Journal of Cybersecurity, 6*(1). Retrieved from: https://doi.org/10.1093/cybsec/tyaa006.

Littleton, H., Grills-Taquechel, A., & Axsom, D. (2009). Resource loss as a predictor of posttrauma symptoms among college women following the mass shooting at Virginia Tech. *Violence and Victims*, *24*(5), 669-686.

Louviere, J. J., Hensher, D. A., & Swait, J. D. (2000). *Stated choice methods: Analysis and applications*. Cambridge University Press.

Ludwig, J. & Cook, P.J. (2001). "The benefits of reducing gun violence: Evidence from contingent-valuation survey data." *Journal of Risk and Uncertainty* 22(3): 207-226.

Lugo, K. & Przybylski, R. (2018). Estimating the financial costs of crime victimization. Justice Research and Statistics Association. Washington, DC: National Criminal Justice Reference Service. Retrieved from: https://www.ojp.gov/pdffiles1/nij/grants/254011.pdf

MacAllister, J. M. (2017). The doxing dilemma: Seeking a remedy for the malicious publication of personal information. Fordham Law Review, 85(5), 2451. Retrieved from: https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article55370&context5flr

Madero-Hernandez, A. (2019). Lifestyle Exposure Theory of Victimization. In F. B. Bernat (ed.), *The Encyclopedia of Women and Crime*, 1-3. John Wiley Sons Inc.

Maple, C., Short, E., Brown, E., Bryden, C., & Salter, M. (2012). Cyberstalking in the UK: Analysis and Recommendations. *International Journal of Distributed Systems and Technologies (IJDST)*, 3(4), 34–51.

Marganski, A., & Melander, L. (2015). Intimate partner violence victimization in the cyber and real world: Examining the extent of cyber aggression experiences and its association with in-person dating violence. *Journal of Interpersonal Violence*, *33*, 1071-1095.

Marganski, A., & Melander, L. (2018). Intimate partner violence victimization in the cyber and real world: Examining the extent of cyber aggression experiences and its association with in-person dating violence. *Journal of Interpersonal Violence*, *33*, 1071-1095.

Marques, O. , & Rinaldi, J. (2020). *The politics of consent and the problem with focusing on violence*. In G. C. Becker , & A. T. Dionne (Eds.), Rape culture 101: Programming change (pp. 128–147). Brantford, ON: Demeter.

Martinez-Pecino, R., & Durán, M. (2019). I love you but I cyberbully you: The role of hostile sexism. *Journal of Interpersonal Violence*, *34*, 812–825.

Marwick, A. E., & Miller, R. W. (2014). *Online harassment, defamation, and hateful speech: A primer of the legal landscape*. Fordham Center on Law and Information Policy Report, (2).

Matthews, T., O'Leary, K., Turner, A., Sleeper, M., Woelfer, J. P., Shelton, M., Manthorne, C., Churchill, E. F., & Consolvo, S. (2017). Security and Privacy Experiences and Practices of Survivors of Intimate Partner Abuse. IEEE Security & Privacy, 15(5), 76–81.

Mayer-Schönberger, V. (2009). *Delete: The Virtue of Forgetting in the Digital Age*. Princeton, NJ: Princeton University Press.

McGlynn, C., Johnson, K., Rackley, E., Henry, N., Gavey, N., Flynn, A., & Powell, A. (2021). 'It's torture for the soul': The harms of image-based sexual abuse. *Social & Legal Studies*, *30*(4), 541-562.

McGlynn, C., & Rackley, E. (2017). Image-based sexual abuse. *Oxford Journal of Legal Studies*, *37*(3), 534-561.

McGlynn, C., & Rackley, E. (2016). *Image-based sexual abuse: More than just 'revenge porn.'* University of Birmingham, United Kingdom.

McGlynn, C., Rackley, E., & Houghton, R. (2017). Beyond 'revenge porn': The continuum of image-based sexual abuse. *Feminist legal studies*, *25*(1), 25-46.

McLean, G. & Bocinski, S. G. (2017). The Economic Cost of Intimate Partner Violence, Sexual Assault, and Stalking: Fact Sheet. Institute for Women's Policy Research. Retrieved from: https://iwpr.org/wp-content/uploads/2017/08/B367_Economic-Impacts-of-IPV-08.14.17.pdf

Mehari, K. R., Thompson, E. L., & Farrell, A. D. (2020). Differential longitudinal outcomes of in-person and cyber victimization in early adolescence. *Psychology of violence*, *10*(4), 367-378.

Messner, S. F., & Blau, J. R. (1987). Routine leisure activities and rates of crime: A macro-level analysis. *Social forces*, *65*(4), 1035-1052.

Miethe, T. D., & Meier, R. F. (1994). *Crime and its social context: Toward an integrated theory of offenders, victims, and situations*. New York: Suny Press.

Miller, T.R., Cohen, M.A. & Rossman, S. (1993). "Victim costs of violent crime and resulting injuries." *Health Affairs 12*(4): 186-197.

Miller, T.R., Cohen, M.A. & Wiersema, B. (1996). *Victim Costs and Consequences: A New Look*. Washington, DC: U.S. Department of Justice, National Institute of Justice.

Miller, T. R., Cohen, M. A., Swedler, D. I., Ali, B., & Hendrie, D. V. (2021). Incidence and Costs of Personal and Property Crimes in the USA, 2017. *Journal of Benefit-Cost Analysis*, *12*(1), 24-54.

Morgan, R. E., & Truman, J. L. (2022). *Stalking victimization, 2019*. NCJ 301735. Bureau of Justice Statistics. Retrieved from: https://bjs.ojp.gov/content/pub/pdf/sv19.pdf.

Mumford, E. A., Maitra, P., Sheridan, J., Rothman, E. F., Olsen, E., & Roberts, E. (2023). Technology-facilitated abuse of young adults in the United States: A latent class analysis. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *17*, Article 7.

National Conference of State Legislators (2016). *Cyber misbehavior*. U.S. Department of Justice: Washington, DC.

National Institute of Justice (2020, November 20). "Ranking Needs for Fighting Digital Abuse: Sextortion, Swatting, Doxing, Cyberstalking and Nonconsensual Pornography." Retrieved from: https://nij.ojp.gov/topics/articles/ranking-needs-fighting-digital-abuse-sextortion-swatting-doxing-cyberstalking

National Network to End Domestic Violence (NNEDV). (2018, September 4). Tech abuse: Information from the field, survey findings from the Conference on Crimes Against Women. Retrieved from: https://www.techsafety.org/blog/2018/9/12/tech-abuse-information-from-the-field.

National Network to End Domestic Violence (NNEDV). 2021. Tech abuse in the pandemic & beyond: Reflections from the field. Retrieved from: https://www.techsafety.org/needs-assessment-2021.

National Resource Center on Domestic Violence. (2021). *Technology-facilitated abuse*. Retrieved from: https://vawnet.org/sc/technology-assisted-abuse.

129

Navarro, J. N., & Jasinski, J. L. (2012). Going cyber: Using routine activities theory to predict cyberbullying experiences. *Sociological Spectrum*, *32*, 81-94.

Nobles, M. R., Reyns, B. W., Fox, K. A., & Fisher, B. S. (2014). Protection against pursuit: A conceptual and empirical comparison of cyberstalking and stalking victimization among a national sample. *Justice Quarterly*, *31*(6), 986-1014.

NORC (2022). *CARI key findings brief.* Retrieved from: https://static1.squarespace.com/static/51dc541ce4b03ebab8c5c88c/t/634845e014a0a73f9 d1098a2/1665680864438/CARI+Key+Findings+Brief.pdf.

Ozer, E. J., Best, S. R., Lipsey, T. L., & Weiss, D. S. (2003). Predictors of posttraumatic stress disorder and symptoms in adults: a meta-analysis. *Psychological bulletin*, *129*(1), 52.

Paroline v. United States – 572 U.S. 434, 134 S. Ct. 1710 (2014). Retrieved from: https://www.lexisnexis.com/community/casebrief/p/casebrief-paroline-v-united-states#:~:text=United%20States%20%2D%20572%20U.S.%20434,1710%20(2014)

Patel, U., & Roesch, R. (2020). The prevalence of technology-facilitated sexual violence: A meta-analysis and systematic review. *Trauma, Violence, & Abuse*, *23*, 428-443.

Peterson, C., & Kearns, M. C. (2021). Systematic Review of Violence Prevention Economic Evaluations, 2000–2019. *American journal of preventive medicine*. Retrieved from: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7987799/

Picasso, E. & Cohen, M.A. (2019). Valuing the public's demand for crime prevention programs: A discrete choice experiment. *Journal of Experimental Criminology*, 15(4): 529-50.

Pina, A., Storey, J. E., Duggan, M., & Franqueira, V.N. (2021). Technology-Facilitated Intimate Partner Violence: A multidisciplinary examination of prevalence, methods used by perpetrators and the impact of COVID-19.

Piquero, N.L., Cohen, M.A. & Piquero, A.R. (2011). How much is the public willing to pay to be protected from identity theft? *Justice Quarterly, 28*(3), 437-458.

Powell, A., & Henry, N. (2019). Technology-facilitated sexual violence victimization: Results from an online survey of Australian adults. *Journal of Interpersonal Violence*, *34*(17), 3637-3665.

Rakotonarivo, O. S., Schaafsma, M., & Hockley, N. (2016). A systematic review of the reliability and validity of discrete choice experiments in valuing non-market environmental goods. *Journal of environmental management*, *183*, 98-109.

Raskolnikov, A. (2020). Criminal deterrence: A review of the missing literature. *Supreme Court Economic Review*, *28*(1), 1-59.

Reed, L. A., Tolman, R. M., & Ward, L. M. (2016). Snooping and sexting: Digital media as a context and tool for dating violence among college students. *Violence Against Women, 22*, 1556–1576.

Reyns, B. (2015). A routine activity perspective on online victimization: Results from the Canadian general social survey. *Journal of Financial Crime, 22*(4), 396–411.

Reyns, B. W., & Fisher, B. S. (2018). The relationship between offline and online stalking

victimization: A gender-specific analysis. *Violence and victims*, *33*(4), 769-786.

Reyns, B. W., Fisher, B. S., & Randa, R. (2018). Explaining cyberstalking victimization against college women using a multitheoretical approach: Self-control, opportunity, and control balance. *Crime & Delinquency*, *64*, 1742-1764.

Reyns, B. W., & Fissel, E. R. (2020). Cyberstalking. In T. Holt and A. Bossler (eds.), *The Palgrave handbook of international cybercrime and cyberdeviance*, 1283-1306. Cham: Palgrave Macmillan.

Reyns, B. W., Henson, B., & Fisher, B. S. (2012). Stalking in the twilight zone: Extent of cyberstalking victimization and offending among college students. *Deviant Behavior*, *33*(1), 1–25.

Rothman, E. F., Sheridan-Johnson, J., Maitra, P., Shulruff, T., Sniffen, C. K., & Mumford, E. A. (2023). Stress, suicidality, post-traumatic stress disorder, emotional distress, and social isolation among U.S. adults experiencing online abuse or harassment. *Violence and Gender*, *10*, 144-152.

Ruvalcaba, Y., & Eaton, A. A. (2019). Nonconsensual pornography among U.S. adults: A sexual scripts framework on victimization, perpetration, and health correlates for women and men. *Psychology of Violence*, *10*, 68-78.

Safety Net Project. (2021). Tech Abuse in the Pandemic & Beyond: Reflections from the Field. National Network to End Domestic Violence. https://www.techsafety.org/needs-assessment-2021.

Sambasivan, N., Batool, A., Ahmed, N., Matthews, T., Thomas, K., Gaytán-Lugo, L. S., ... & Consolvo, S. (2019, May). " 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* (pp. 1-14).

Sauber, E. W., & O'Brien, K. M. (2020). Multiple losses: The psychological and economic well-being of survivors of intimate partner violence. *Journal of interpersonal violence*, *35*(15-16), 3054-3078.

Schuman, H., & Presser, S. (1981). The attitude-action connection and the issue of gun control. *The Annals of the American Academy of Political and Social Science*, *455*(1), 40-47.

Smith, S.G., Basile, K.C., & Kresnow, M. (2022). *The National Intimate Partner and Sexual Violence Survey: 2016/2017 Report on Stalking — Updated Release*. Atlanta, GA: National Center for Injury Prevention and Control, Centers for Disease Control and Prevention.

Stanley, N., Barter, C., Wood, M., Aghtaie, N., Larkins, C., Lanau, A., & Overlien, C. (2018). Pornography, sexual coercion and abuse and sexting in young people's intimate relationships: A European study. *Journal of Interpersonal Violence*, *33*, 2919-2944.

Stevens, F., Nurse, J. R., & Arief, B. (2021). Cyber stalking, cyber harassment, and adult mental health: A systematic review. *Cyberpsychology, Behavior, and Social Networking*, *24*(6), 367-376.

Stokey, E. & Zeckhauser, R. (1978). *A primer for policy analysis*. W.W. Norton & Company.

Stonard, K., Bowen, E., Lawrence, T., & Price, S.A. (2014). The relevance of technology to the nature, prevalence and impact of adolescent dating violence and abuse: A research synthesis. *Aggression and Violent Behavior,* 19, 390–417.

Sullivan, C. M. (2016). Examining the work of domestic violence programs within a "social and emotional well-being promotion" conceptual framework. National Resource Center on Domestic Violence. Retrieved from: https://www.dvevidenceproject.org/wp-content/uploads/DVEvidenceServices-ConceptualFramework-2016.pdf

Sullivan, C. M. (2018). Understanding how domestic violence support services promote survivor wellbeing: A conceptual model. Journal of Family Violence, 33(2), 123–131.

Taylor, S., & Xia, Y. (2018). Cyber partner abuse: A systematic review. *Violence and victims*, *33*(6), 983-1011.

Tennant, J. E., Demaray, M. K., Coyle, S., & Malecki, C. K. (2015). The dangers of the web: Cybervictimization, depression, and social support in college students. *Computers in Human Behavior*, *50*, 348-357.

Tinelli, M. (2016). Applying discrete social experiments in social care research. *Method Reviews: LSE Research Online.*

Tompson, L., Belur, J., & Jerath, K. (2021). A victim-centred cost–benefit analysis of a stalking prevention programme. *Crime Science, 10.* Retrieved from: https://doi.org/10.1186/s40163-021-00158-5

Trickey, D., Siddaway, A. P., Meiser-Stedman, R., Serpell, L., & Field, A. P. (2012). A meta-analysis of risk factors for post-traumatic stress disorder in children and adolescents. *Clinical psychology review*, *32*(2), 122-138.

Truman, J., & Morgan, R. (2021). *Stalking Victimization, 2016*. NCJ 253526. Bureau of Justice Statistics. Retrieved from: https://bjs.ojp.gov/redirect-legacy/content/pub/pdf/sv16.pdf

Ullman, S. E. (2010). Talking about sexual assault: Society's response to survivors. *American Psychological Association* Retrieved from: http://www.apa.org/pubs/books/4318073.aspx.

United States Department of Justice. (2016). Cyber Misbehavior, 64(3). Retrieved from: www.justice.gov/usao/file/851856/download

Vakhitova, Z. I., Alston-Knox, C. L., Reeves, E., & Mawby, R. I. (2021). Explaining victim impact from cyber abuse: An exploratory mixed methods analysis. *Deviant Behavior*, 1-20.

Vakhitova, Z. I., Reynald, D. M., & Townsley, M. (2016). Toward the adaptation of routine activity and lifestyle exposure theories to account for cyber abuse victimization. *Journal of Contemporary Criminal Justice*, *32*(2), 169-188.

Van Ouytsel, J., Ponnet, K., & Walrave, M. (2020). Cyber dating abuse: Investigating digital monitoring behaviors among adolescents from a social learning perspective. *Journal of interpersonal violence*, *35*(23-24), 5157-5178.

Vogler, S., Kappel, R., & Mumford, E. (2023). Experiences of technology-facilitated abuse among sexual and gender minorities. *Journal of Interpersonal Violence*, *38*, 11290-11313.

Ybarra, M., Price-Feeney, M., Lenhart, A., & Zickuhr, K. (2017). Intimate partner digital abuse. *Center for Innovative Public Health Research.* Retrieved from: https://innovativepublichealth. org/publications/intimate-partner-digital-abuse/

Vilk, V., Bailey, M., Lopez, S., & Nossel, S. (2021). *No Excuse for Abuse: What Social Media Companies Can Do Now to Combat Online Harassment and Empower Users.* PEN America. Retrieved from: https://pen.org/report/no-excuse-for-abuse/

Waldman, A. E. (2019). Law, privacy, and online dating: "Revenge porn" in gay online communities. *Law & Social Inquiry*, *44*(4), 987-1018.

Walker, K., & Sleath, E. (2017). A systematic review of the current knowledge regarding revenge pornography and non-consensual sharing of sexually explicit media. *Aggression and Violent Behavior*, *36*, 9-24.

Walker, K., Sleath, E., Hatcher, R. M., Hine, B., & Crookes, R. L. (2019). Nonconsensual sharing of private sexually explicit media among university students. *Journal of Interpersonal Violence*, *36*, NP9078-NP9108.

Wilson, C., Sheridan, L., & Garratt-Reed, D. (2022). What is cyberstalking? A review of measurements. *Journal of Interpersonal Violence*, *37*(11-12), 9763-9783.

Wilson, C., Sheridan, L., & Garratt-Reed, D. (2023). Examining cyberstalking perpetration and victimization: A scoping review. *Trauma, Violence, & Abuse*, *24*, 2019-2033.

Witwer, A. R., Langton, L., Vermeer, M. J. D., Banks, D., Woods, D., & Jackson, B. A. (2020). *Countering Technology-Facilitated Abuse: Criminal Justice Strategies for Combating Nonconsensual Pornography, Sextortion, Doxing, and Swatting*. Santa Monica, CA: RAND Corporation. Retrieved from: https://www.rand.org/pubs/research_reports/RRA108-3.html.

Wood, M., Barter, C., Stanley, N., Aghtaie, N., & Larkins, C. (2015). Images across Europe: The sending and receiving of sexual images and associations with interpersonal violence in young people's relationships. *Children and Youth Services*, *59*, 149-160.

Woodlock, D. (2017). The abuse of technology in domestic violence and stalking. *Violence against Women*, *23*(5), 584-602.

Woodlock, D., McKenzie, M., Western, D., & Harris, B. (2020). Technology as a weapon in domestic violence: Responding to digital coercive control. Australian social work, 73(3), 368-380.

Wright, M. F., & Li, Y. (2013). The association between cyber victimization and subsequent cyber aggression: The moderating effect of peer rejection. *Journal of youth and adolescence*, *42*(5), 662-674.

Yar, M. (2005). The novelty of 'cybercrime': An assessment in light of routine activity theory. *European Journal of Criminology*, *2*, 407-427.

Yardley, E. (2021). Technology-facilitated domestic abuse in political economy: A new

theoretical framework. *Violence against women*, *27*(10), 1479-1498.

Ybarra, M., Price-Feeney, M., Lenhart, A., & Zickuhr, K. (2017). *Intimate partner digital abuse*. Center for Innovative Public Health Research. Retrieved from: https://innovativepublichealth.org/publications/intimate-partner-digital-abuse

Zweig, J. M., Lachman, P., Yahner, J., & Dank, M. (2014). Correlates of cyber dating abuse among teens. *Journal of youth and adolescence*, *43*(8), 1306-1321.

Appendix 1: Final Survey Instrument

Study Information

CONSENT AND INTRO

BASE: ALL RESPONDENTS

CONSENT100. [DISPLAY]

Thank you very much for participating in KnowledgePanel® surveys. This particular survey asks about different forms of technology-facilitated abuse and will take about 15 minutes to complete.

This survey is being conducted by the Justice Research and Statistics Association and is funded by the U.S. Department of Justice (DOJ). The study will help researchers understand how the general public values solving this problem as well as the harms that people suffer because of it. This information will help service providers and policy makers to better help people who experience this kind of abuse.

As with all KnowledgePanel® surveys, responding to this survey, or to any individual question on the survey, is completely voluntary. De-identified data from this study will be archived with the National Archive of Criminal Justice Data as required for DOJ-funded studies by US code 28 CFR §22.23(b)(4). Your responses will remain anonymous and will only be used for research analyses.

If you have questions about your rights as a participant in this survey, or if you are dissatisfied at any time with any aspect of the survey, you may contact KnowledgePanel Member Support at 800-782-6899.

If you consent to participate in this study, please click the forward button below to begin the survey.

BASE: ALL RESPONDENTS

INTRO100. [DISPLAY]

In this survey, we will ask questions about three forms of technology-facilitated abuse—cyberstalking, doxing, and image-based sexual abuse. These abuses can be associated with the following:

- Victims might suffer psychological distress, such as anxiety, depression, embarrassment, shame, damage to reputation, or fear of future victimization.
- Victims might have to spend money to repair the damage, such as legal fees, relocation expenses, therapy costs, and so on.

BASE: ALL RESPONDENTS

DOV_SECTION1. [HIDDEN VARIABLE – RANDOMLY SELECT 1 FOR FIRST SECTION]

1. ISBA – image-based sexual abuse
2. DOX – doxing
3. STALK – cyberstalking

DOV_SECTION2. [HIDDEN VARIABLE – KEEP 2 CODES NOT SELECTED IN DOV_SECTION1 AND RANDOMLY SELECT 1 FOR SECOND SECTION]

1. ISBA – image-based sexual abuse
2. DOX – doxing
3. STALK – cyberstalking

BASE: ALL RESPONDENTS

DOV_SECTION3. [HIDDEN VARIABLE – SELECT CODE NOT SELECTED AT DOV_SECTION1 AND DOV_SECTION2]

1. ISBA – image-based sexual abuse
2. DOX – doxing
3. STALK – cyberstalking

PROGRAMMING: DOV_SECTION1 IS PRESENTED FIRST, DOV_SECTION2 IS PRESENTED SECOND, AND DOV_SECTION3 IS PRESENTED THIRD.

PROGRAMMING: PRESENT IMAGE-BASED SEXUAL ABUSE SECTION IN ORDER BASED ON DOV_SECTION1=1, DOV_SECTION2=1, OR DOV_SECTION3=1.

IMAGE-BASED SEXUAL ABUSE

BASE: ALL RESPONDENTS

IBSA100. [S] [IF DOV_SECTION2=1 OR DOV_SECTION3=1 INSERT Next, we have another topic we want to ask you about.**]**

Sometimes people threaten to share or actually share images or videos of others that are partially nude, nude, or sexually explicit without the consent of people in the images. These images could be real, faked, or altered. This is called **image-based sexual abuse**.

Regardless of whether or not the images or videos were actually shared, has anyone ever **threatened** to share real or fake partially nude, nude, or sexually explicit images or videos of you without your consent?

1. Yes
2. No

PROGRAMMER: Please add the following text under the next button in smaller font (-1 font size) on the same screen as IBSA100.

If you need help or are experiencing distress, please contact the National Domestic Violence Hotline at 1-800-799-7233 or online.

BASE: ALL RESPONDENTS

IBSA110. [S] Regardless of whether or not you were threatened, has anyone ever **actually shared or posted** any real or fake partially nude, nude, or sexually explicit images or videos of you without your consent?

1. Yes
2. No

BASE: IBSA100=1 AND IBSA110=1

IBSA115. [S] Was the person who first shared or posted the images or videos of you the same person who threatened you?

1. Yes
2. No

BASE: ALL RESPONDENTS

DOV_IBSA. [HIDDEN QUESTION – ASSIGN CODE]

PROGRAMMER: If IBSA100=1 or IBSA110=1, get code 1. Else get code 0.
0. Did not experience IBSA
1. Experienced IBSA

BASE: DOV_IBSA=1

IBSA120. [S] Has image-based sexual abuse happened to you more than once? If other people reshared the same images or videos after the first person shared them, but no *new* images or videos were shared, count this as once.

1. Yes
2. No

BASE: IBSA110=1

IBSA130. [S] [IF IBSA120=1 INSERT: For the rest of these questions, please think about the most recent time that this happened to you.**]** When did you become aware that the images or videos of you were shared or posted?

1. In the past 12 months
2. More than 12 months ago, but after COVID-19 started (since March 2020)
3. Pre-COVID-19 (before March 2020)

BASE: IBSA110=1

IBSA140. [S] When do you think it was originally shared or posted?

1. In the past 12 months
2. More than 12 months ago, but after COVID-19 started (since March 2020)
3. Pre-COVID-19 (before March 2020)

BASE: IBSA100=1

IBSA150. [S] [IF IBSA110 NE 1 AND IBSA120=1 INSERT: For the rest of these questions, please think about the most recent time that this happened to you.**]** When were you first threatened about the images or videos of you being shared or posted?

1. In the past 12 months
2. More than 12 months ago, but after COVID-19 started (since March 2020)
3. Pre-COVID-19 (before March 2020)

BASE: IBSA100=1

IBSA160. [BANKED] Were you asked to do the following to prevent the images or videos from being shared?

PROGRAMMER: Randomize and record the order of statements A-D
Statements:
   A. Send money or cryptocurrency
   B. Send more nude or sexually explicit images or videos
   C. Do something sexual for them
   D. Stay in a romantic relationship against my wishes
   E. Something else, please specify: **[TEXTBOX, ANCHOR]**

Responses:
   1. Yes
   2. No

BASE: IBSA100=1

IBSA170. [BANKED] What happened after they threatened to share your images or videos?

PROGRAMMER: Do NOT randomize statements
Statements:
   A. They eventually stopped bothering me without me doing anything
   B. They made more threats or demands
   C. I contacted the police or other help to try to stop it
   D. **[IF IBSA110=1, INSERT**: I did what they asked me to do and they stopped sharing the images or videos**; IF IBSA110=2 OR REFUSED INSERT**: I did what they asked me to do and they did not share the images or videos**]**
   E. I did what they asked me to do but they still shared the images or videos
   F. The threat is still ongoing
   G. Other, please specify **[TEXTBOX]**

Responses:
1. Yes
2. No
3. Don't know **[display for option F only]**

BASE: IBSA110=1

IBSA180. [BANKED] You indicated that the images or videos of you were shared. How were they shared?

PROGRAMMER: Randomize and record the order of statements A-D
Statements:
A. Sent to others through online messaging apps or texts
B. Posted on social media or other public websites
C. Sent hard-copy images to others through the mail
D. Posted hard-copy images in a public area
E. A different method, please describe: **[TEXTBOX, ANCHOR]**

Responses:
1. Yes
2. No

BASE: IBSA180_A=1 OR IBSA180_C=1

IBSA190. [M] Who directly received the images or videos of you? Please select ALL that apply.

A. Family
B. Friends
C. Coworkers
D. My boss
E. Others **[TEXTBOX]**

BASE: IBSA100=1

IBSA200. [S] Did you see the images or videos that the person threatened to share?

1. Yes
2. No

BASE: IBSA110=1 OR IBSA200=1

IBSA210. [BANKED] [IF IBSA110=1 INSERT: Did the images, videos, or any information shared with them have any of the following that could identify you?**] [IF IBSA110 ne 1 and IBSA200=1 INSERT:** Did the images or videos have any of the following that could identify you?**]**

PROGRAMMER: Randomize and record the order of statements

Statements:

A. My face or identifying tattoos, birthmarks, or other features
B. My name, home or work address, phone number, email address, social media handles, or other identifying information

Responses:

1. Yes
2. No

BASE: IBSA110=1 OR IBSA200=1

IBSA220. [S] Were the images or videos real, faked, or altered?

1. The images were real – for example, real intimate selfies or videos or being secretly photographed or recorded
2. The images were faked or altered – the image was manipulated to look like I was partially nude, nude, or engaged in a sex act in the images
3. There were both real and faked or altered images or videos

BASE: IBSA110=1 OR IBSA200=1

IBSA230. [N] Approximately how old were you when the images or videos were taken?

[NUMERIC BOX, RANGE: 0-120] years old
The image or video did not contain anything real **[EXCLUSIVE]**

BASE: DOV_IBSA=1

IBSA240. [M] How did the person get the images or videos of you? Please select ALL that apply.

A. I gave them to the person voluntarily
B. They photographed or recorded me with my consent
C. They photographed or recorded me **without** my consent
D. Someone else gave them to the person without my consent
E. They found them online
F. They hacked into my smartphone, computer, accounts, or other devices
G. The image or video did not contain anything real
H. Some other way
I. I don't know **[EXCLUSIVE]**

BASE: DOV_IBSA=1

IBSA250. [S] Was there more than one person who shared or threatened to share images or videos of you?

1. Yes
2. No

3. I don't know

IBSA260. [S] **[IF IBSA250=1,3 INSERT:** Please answer the following questions based on the **primary person** you consider responsible for the image-based sexual abuse you experienced.**]** When your images or videos were first shared or threatened to be shared, what was your relationship with the person responsible for this?

1. Dating partner, spouse, or casual intimate partner
2. Ex-dating partner, spouse, or casual intimate partner
3. Family
4. Friend
5. Coworker
6. Acquaintance
7. Stranger
8. Other, please describe: **[TEXTBOX]**
9. I do not know who it was

IBSA270. [S] How did you first meet the person who shared or threatened to share the images or videos of you?

PROGRAMMER: Randomize and record the order of statements 1-4
1. Online
2. School or college
3. Work
4. In my neighborhood
5. Somewhere else **[TEXTBOX, ANCHOR]**

IBSA280. [S] When your images or videos were first shared or threatened to be shared, how long had you known the person responsible for this?

1. Less than a week
2. Less than a month
3. Less than 6 months
4. Less than a year
5. One to two years
6. More than two years

IBSA290. [M] How did you interact with the person **after** they shared or threatened to share the images or videos of you? Please select ALL that apply.

PROGRAMMER: Randomize and record the order of statements A-C
A. Met them in person

B. Talked to them on phone or video chat
C. Talked to them online or through text
D. Did not interact with them at all **[EXCLUSIVE, ANCHOR]**

IBSA300. [S] Did you pay for a service to help you remove the images or videos of you from the internet?

1. Yes
2. No

IBSA310. [S] Were the images or videos of you that were shared ever fully removed from the internet, deleted, or destroyed?

1. Yes
2. No
3. I don't know

IBSA320. [S] How long did it take to fully remove, delete, or destroy the images or videos of you?

1. Less than a week
2. Less than a month
3. Less than 6 months
4. Less than a year
5. One to two years
6. More than two years

PROGRAMMING: PRESENT DOXING SECTION IN ORDER BASED ON DOV_SECTION1=2, DOV_SECTION2=2, OR DOV_SECTION3=2.

DOXING

DOX100. [S] [IF DOV_SECTION2=2 OR DOV_SECTION3=2 INSERT: Next, we have another topic we want to ask you about.**]**

Doxing is when someone releases your personal contact or sensitive information (other than photos or videos) to others without your consent. <u>Note</u>: this does not include mass data breaches, which occur when hackers steal your private information from a credit card company or other data sources.

Has anyone ever doxed you by publicly posting your work/school/home address, phone number, social security number, social media accounts, sexual history, or medical or financial information online without your consent?

1. Yes
2. No

PROGRAMMER: Please add the following text under the next button in smaller font (-1 font size) on the same screen as DOX100.

If you need help or are experiencing distress, please contact the National Domestic Violence Hotline at 1-800-799-7233 or online.

BASE: ALL RESPONDENTS

DOX110. [S] Another form of doxing is inciting others to use your personal information to harass or threaten you through mass phone calls, opening credit cards in your name, creating a cyber mob to attack you, showing up at your house, or some other group harassment. Has this ever happened to you?

1. Yes
2. No

BASE: ALL RESPONDENTS

DOV_DOX. [HIDDEN QUESTION – ASSIGN CODE]

PROGRAMMER: If DOX100=1 OR DOX110=1, get code 1. Else get code 0.

0. Did not experience doxing
1. Experienced doxing

BASE: DOV_DOX=1

DOX120. [S] Has doxing happened to you more than once? If the same person was responsible for this multiple times, please consider this as happening once.

1. Yes
2. No

BASE: DOV_DOX=1

DOX130. [S] [IF DOX120=1 INSERT: For the rest of these questions, please think about the most recent time that this happened to you.**]** When did you become aware that your personal information was shared or posted?

1. In the past 12 months
2. More than 12 months ago, but after COVID-19 started (since March 2020)
3. Pre-COVID-19 (before March 2020)

BASE: DOV_DOX=1

DOX140. [S] When do you think your personal information was originally shared or posted?

1. In the past 12 months
2. More than 12 months ago, but after COVID-19 started (since March 2020)
3. Pre-COVID-19 (before March 2020)

BASE: DOV_DOX=1

DOX150. [BANKED] How was your personal information shared?

PROGRAMMER: Randomize and record the order of statements A-D
Statements:

A. Sent to others through online messaging apps or texts
B. Posted on social media or other public websites
C. Sent hard copies of the information to others through the mail
D. Posted hard copies of the information in a public area
E. A different method, please describe: **[TEXTBOX, ANCHOR]**

Responses:

1. Yes
2. No

BASE: DOX150_A=1 OR DOX150_C=1

DOX160. [M] Who directly received your personal information? Please select ALL that apply.

A. Family
B. Friends
C. Coworkers
D. My boss
E. Others **[TEXTBOX]**

BASE: DOV_DOX=1

DOX170. [S] Was there more than one person who shared your personal information?

1. Yes
2. No
3. I don't know

BASE: DOV_DOX=1

DOX180. [S] [IF DOX170=1,3 INSERT: Please answer the following questions based on the **primary person** you consider responsible for the doxing you experienced.**]** When your personal information was first shared, what was your relationship with the person responsible for this?

1. Dating partner, spouse, or casual intimate partner

144

2. Ex-dating partner, spouse, or casual intimate partner
3. Family
4. Friend
5. Coworker
6. Acquaintance
7. Stranger
8. Other, please describe: **[TEXTBOX]**
9. I do not know who it was

BASE: DOX180 NE 3, 7, 9, REFUSED OR SKIP

DOX190. [S] How did you first meet the person who shared your personal information?

PROGRAMMER: Randomize and record the order of statements 1-4
1. Online
2. School or college
3. Work
4. In my neighborhood
5. Somewhere else **[TEXTBOX, ANCHOR]**

BASE: DOX180 NE 7, 9, REFUSED OR SKIP

DOX200. [S] When your personal information was first shared, how long had you known the person responsible for this?

1. Less than a week
2. Less than a month
3. Less than 6 months
4. Less than a year
5. One to two years
6. More than two years

BASE: DOV_DOX=1

DOX210. [M] How did you interact with the person **after** they shared your personal information? Please select ALL that apply.

PROGRAMMER: Randomize and record the order of statements A-C
A. Met them in person
B. Talked to them on the phone or through video chat
C. Talked to them online or through text
D. Did not interact with them at all **[EXCLUSIVE, ANCHOR]**

BASE: DOX150_A=1 OR DOX150_B=1

DOX220. [S] Did you pay for a service to help you remove your personal information that was shared from the internet?

1. Yes
2. No

DOX230. [S] Was the personal information that was shared ever fully removed from the internet, deleted, or destroyed?

1. Yes
2. No
3. I don't know

DOX240. [S] How long did it take to fully remove, delete, or destroy your personal information that was shared?

1. Less than a week
2. Less than a month
3. Less than 6 months
4. Less than a year
5. One to two years
6. More than two years

PROGRAMMING: PRESENT CYBERSTALKING SECTION IN ORDER BASED ON DOV_SECTION1=3, DOV_SECTION2=3, OR DOV_SECTION3=3.

CYBERSTALKING

STALK100. [S] [IF DOV_SECTION2=3 OR DOV_SECTION3=3 INSERT: Next, we have another topic we want to ask you about.]**

Sometimes people use technology to repeatedly harass another person, spy on them, or monitor or interfere with their activity. This is called **cyberstalking**. Has anyone ever done this to you?

1. Yes
2. No

PROGRAMMER: Please add the following text under the next button in smaller font (-1 font size) on the same screen as STALK100.

If you need help or are experiencing distress, please contact the National Domestic Violence Hotline at 1-800-799-7233 or online.

BASE: ALL RESPONDENTS

DOV_STALK. [HIDDEN QUESTION – ASSIGN CODE]

PROGRAMMER: If STALK100=1, get code 1. Else get code 0.
  0. Did not experience cyberstalking
  1. Experienced cyberstalking

BASE: DOV_STALK=1

STALK110. [BANKED] There are many types of cyberstalking. Did you experience the following?

PROGRAMMER: Randomize and record the order of statements
Statements:
  A. I received unwanted and repeated texts, emails, or social media messages (does not include spam or phishing emails or texts)
  B. Someone monitored my social media, email, financial, or other accounts and communications to track my activities
  C. Someone installed stalkerware or spyware on my phone or computer (such as a key logger)
  D. Someone changed my login information or security settings on my devices or social media accounts
  E. Someone impersonated me to interfere with my personal or work relationships, cancel important events (like court dates), or run up debts
  F. Someone tracked my location using technology (such as a GPS tracker, mobile phone, digital doorbell)
  G. Someone watched me using devices that I did not know about

Responses:
  1. Yes
  2. No

BASE: DOV_STALK=1

STALK120. [S] Has cyberstalking happened to you more than once? If the same person was responsible for this multiple times, please consider this as happening once.

  1. Yes
  2. No

BASE: DOV_STALK=1

STALK130. [S] [IF STALK120=1, INSERT: For the rest of these questions, please think about the most recent time that this happened to you.**]** When did you become aware that someone was cyberstalking you?

1. In the past 12 months
2. More than 12 months ago, but after COVID-19 started (since March 2020)
3. Pre-COVID-19 (before March 2020)

BASE: DOV_STALK=1

STALK140. [S] When do you think the cyberstalking originally began?

1. In the past 12 months
2. More than 12 months ago, but after COVID-19 started (since March 2020)
3. Pre-COVID-19 (before March 2020)

BASE: DOV_STALK=1

STALK150. [S] Is the cyberstalking still ongoing?

1. Yes
2. No
3. I don't know

BASE: STALK150=2

STALK160. [N] How long did the cyberstalking last?

[NUMERIC BOX, RANGE: 0-12] months   [NUMERIC BOX, RANGE: 0-24] years

BASE: DOV_STALK=1

STALK170. [S] Was there more than one person who cyberstalked you?

1. Yes
2. No
3. I don't know

BASE: DOV_STALK=1

STALK180. [S] [IF STALK170=1,3 INSERT: Please answer the following questions based on the **primary person** you consider responsible for the cyberstalking you experienced.**]** When the cyberstalking began, what was your relationship with the person responsible for this?

1. Dating partner, spouse, or casual intimate partner
2. Ex-dating partner, spouse, or casual intimate partner
3. Family
4. Friend
5. Coworker
6. Acquaintance

148

7. Stranger
8. Other, please describe: **[TEXTBOX]**
9. I do not know who it was

BASE: STALK180 NE 3, 7, 9, REFUSED OR SKIP

STALK190. [S] How did you first meet the person who cyberstalked you?

PROGRAMMER: Randomize and record the order of statements 1-4

1. Online
2. School or college
3. Work
4. In my neighborhood
5. Somewhere else **[TEXTBOX, ANCHOR]**

BASE STALK180 NE 7, 9, REFUSED OR SKIP

STALK200. [S] When the cyberstalking began, how long had you known the person responsible for this?

1. Less than a week
2. Less than a month
3. Less than 6 months
4. Less than a year
5. One to two years
6. More than two years

BASE: DOV_STALK=1

STALK210. [M] How did you interact with the person **after** you learned of their activities? Please select ALL that apply.

PROGRAMMER: Randomize and record the order of statements A-C

A. Met them in person
B. Talked to them on phone or video chat
C. Talked to them online or through text
D. Did not interact with them at all **[EXCLUSIVE, ANCHOR]**

BASE: DOV_STALK=1

STALK220. [M] Who was aware that you were being cyberstalked? Please select ALL that apply.

A. Family
B. Friends
C. Coworkers
D. My boss
E. Others **[TEXTBOX]**

    F. No one **[EXCLUSIVE]**

HARMS

BASE: ALL RESPONDENTS
DOV_ABUSE. [HIDDEN QUESTION – ASSIGN CODE]

PROGRAMMING: If DOV_IBSA=1 or DOV_DOX=1 or DOV_STALK=1, assign code 1. Else assign code 0.
    0. Did not experience any abuse
    1. Experienced at least one abuse

BASE: DOV_ABUSE=1
DOV_ABUSE_TYPE. [HIDDEN QUESTION – ASSIGN CODE]

PROGRAMMING:
If DOV_IBSA=1 and DOV_DOX=0 and DOV_STALK=0, assign code 1.
If DOV_IBSA=0 and DOV_DOX=1 and DOV_STALK=0, assign code 2.
If DOV_IBSA=0 and DOV_DOX=0 and DOV_STALK=1, assign code 3.
If DOV_IBSA=1 and DOV_DOX=1 and DOV_STALK=0, assign code 4.
If DOV_IBSA=1 and DOV_DOX=0 and DOV_STALK=1, assign code 5.
If DOV_IBSA=0 and DOV_DOX=1 and DOV_STALK=1, assign code 6.
If DOV_IBSA=1 and DOV_DOX=1 and DOV_STALK=1, assign code 7.

    1. image-based sexual abuse
    2. doxing
    3. cyberstalking
    4. image-based sexual abuse and/or doxing
    5. image-based sexual abuse and/or cyberstalking
    6. doxing and/or cyberstalking
    7. image-based sexual abuse, doxing, and/or cyberstalking

BASE: DOV_ABUSE=1
HARM_SCHOOL. [S] Were you a student at any time when you experienced the [INSERT DOV_ABUSE_TYPE]?

    1. Yes
    2. No

BASE: DOV_ABUSE=1
HARM_WORK. [S] Were you employed at any time when you experienced the [INSERT DOV_ABUSE_TYPE]?

1. Yes
2. No

HARM_SMALLBUS. [S] Did you own a business at any time when you experienced the [INSERT DOV_ABUSE_TYPE]?

1. Yes
2. No

BASE: DOV_ABUSE=1

HARM100 (Physical Safety). [BANKED] Next, we'd like to ask you about some things you may have experienced due to these events.

Did the following happen to you because of the [INSERT DOV_ABUSE_TYPE] you experienced?

Statements:
A. I was physically threatened
B. I was physically harmed
C. Someone close to me was physically threatened or harmed
D. My property was destroyed or vandalized
E. Someone trespassed on my property
F. I had to move from where I was living

Responses:
1. Yes
2. No

BASE: HARM100_D=1

HARM110_D. [S] About how much was the value of the property that was destroyed or vandalized?

1. $0
2. $1 to $500
3. $501 to $1,000
4. $1,001 to $5,000
5. $5,001 to $10,000
6. $10,001 to $50,000
7. $50,001 or more
8. Don't know

BASE: HARM100_F=1

151

This resource was prepared by the author(s) using Federal funds provided by the U.S. Department of Justice. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

HARM110_F. [S] About how much did it cost you to move? Please include costs such as breaking a rental lease, paying a rental deposit, hiring movers, selling or buying a home, and so on.

1. $0
2. $1 to $500
3. $501 to $1,000
4. $1,001 to $5,000
5. $5,001 to $10,000
6. $10,001 to $50,000
7. $50,001 or more
8. Don't know

BASE: DOV_ABUSE=1

HARM200 (Health). [BANKED] Did the following happen to you, or get worse, because of the [INSERT DOV_ABUSE_TYPE] you experienced?

Statements:
A. I developed substance dependency or it worsened
B. I felt anxious, sad, unsafe, trapped, or another distressing feeling
C. I had thoughts about ending my life
D. I lost support from family, friends, or other people
E. I was blamed for what happened
F. I got mental health care, including therapy, medicines, or so on
G. I had problems with my physical health (headaches, lack of sleep, nausea, and so on)
H. I got medical care for my physical health problems, including healthcare visits, medicines, or so on

Responses:
1. Yes
2. No

BASE: HARM200_F=1

HARM210_F. [S] About how much were your out-of-pocket expenses for mental health care?

1. $0
2. $1 to $500
3. $501 to $1,000
4. $1,001 to $5,000
5. $5,001 to $10,000
6. $10,001 to $50,000
7. $50,001 or more
8. Don't know

BASE: HARM200_F=1

HARM220_F. [S] Did you have additional costs for mental health care that were covered by other sources (such as health insurance, family members, victim assistance programs)?

1. Yes
2. No

BASE: HARM200_F=1

HARM230_F. [S] Are you still receiving mental health care because of the [INSERT DOV_ABUSE_TYPE] you experienced?

1. Yes
2. No

BASE: HARM200_H=1

HARM210_H. [S] About how much were your out-of-pocket medical expenses for your physical health problems?

1. $0
2. $1 to $500
3. $501 to $1,000
4. $1,001 to $5,000
5. $5,001 to $10,000
6. $10,001 to $50,000
7. $50,001 or more
8. Don't know

BASE: HARM200_H=1

HARM220_H. [S] Did you have additional medical costs for your physical health problems that were covered by other sources (such as health insurance, family members, victim assistance programs)?

1. Yes
2. No

BASE: HARM200_H=1

HARM230_H. [S] Are you still continuing to get medical care for your physical health problems because of the [INSERT DOV_ABUSE_TYPE] you experienced?

1. Yes
2. No

BASE: DOV_ABUSE=1

153

HARM300 (Technology). [BANKED] Did the following happen to you because of the [INSERT DOV_ABUSE_TYPE] you experienced?

Statements:
    A. I closed my accounts on apps or websites or stopped using them
    B. I opened new accounts on apps or websites to replace the old accounts
    C. I was locked out of my devices or accounts
    D. I felt nervous or frightened using my existing accounts on apps or websites
    E. I bought a new or replacement phone, tablet, computer, or similar device
    F. I bought a new or replacement internet-connected or smart home device (such as a security system, baby monitor)

Responses:
    1. Yes
    2. No

BASE: HARM300_A=1 OR HARM300_B=1

HARM310_AB. [S] About how much did it cost you to close old accounts or open new accounts?

    1. $0
    2. $1 to $500
    3. $501 to $1,000
    4. $1,001 to $5,000
    5. $5,001 to $10,000
    6. $10,001 to $50,000
    7. $50,001 or more
    8. Don't know

BASE: HARM300_E=1 OR HARM300_F=1

HARM310_EF. [S] About how much did it cost you to buy new or replacement devices (such as phone, computer, security system)?

    1. $0
    2. $1 to $500
    3. $501 to $1,000
    4. $1,001 to $5,000
    5. $5,001 to $10,000
    6. $10,001 to $50,000
    7. $50,001 or more
    8. Don't know

HARM400 (Educational). [BANKED] Did the following happen to you, or get worse, because of the [INSERT DOV_ABUSE_TYPE] you experienced?

Statements:
  A. I had a hard time focusing at school or on my schoolwork
  B. I missed days of school
  C. I took an extended break from school
  D. I dropped out of school
  E. I was expelled from school
  F. I was punished in some other way by the school
  G. [IF DOV_IBSA=1 OR DOV_DOX=1, INSERT My private information or images of me were seen by people in the school community]

Responses:
  1. Yes
  2. No

HARM410_B. [N] About how many days of school did you miss?

[NUMERIC BOX, RANGE: 0 TO 180] days of school

HARM410_CDE. [S] About how much money, if any, did you lose as a result of taking an extended break from school, dropping out of school, or being expelled from school?

  1. $0
  2. $1 to $500
  3. $501 to $1,000
  4. $1,001 to $5,000
  5. $5,001 to $10,000
  6. $10,001 to $50,000
  7. $50,001 or more
  8. Don't know

HARM500 (Professional). [BANKED] Did the following happen to you, or get worse, because of the [INSERT DOV_ABUSE_TYPE] you experienced?

Statements:
  A. I had a hard time focusing on my job
  B. **[IF DOV_IBSA=1 OR DOV_DOX=1, INSERT:** My private information or images of me were seen by people I work with]
  C. I missed days of work using <u>paid</u> time off
  D. I missed days of work using <u>unpaid</u> time off

155

E. Someone in my family missed work
F. I quit my job
G. I was fired from my job
H. I was turned down for a promotion
I. I missed out on a new job opportunity
J. [IF HARM_SMALLBUS=1, INSERT I closed the comment section on web pages related to the small business that I own]
K. [IF HARM_SMALLBUS=1, INSERT I stopped using web pages related to the small business that I own]

Responses:
1. Yes
2. No

BASE: HARM500_C=1

HARM510_C. [N] About how many days of <u>paid</u> time off did you take?

[NUMERIC BOX, RANGE: 0 TO 365] days of paid time off

BASE: HARM500_D=1

HARM510_D. [N] About how many days of <u>unpaid</u> time off did you take?

[NUMERIC BOX, RANGE: 0 TO 365] days of unpaid time off

BASE: HARM510_C>0

HARM520_C. [S] About how much money did you lose from your <u>unpaid</u> time off?

1. $0
2. $1 to $500
3. $501 to $1,000
4. $1,001 to $5,000
5. $5,001 to $10,000
6. $10,001 to $50,000
7. $50,001 or more
8. Don't know

BASE: HARM500_F=1 OR HARM500_G=1

HARM510_FG. [N] About how many days were you unemployed after you quit or got fired?

[NUMERIC BOX, RANGE: 0 TO 999] days unemployed

BASE: HARM500_F=1 OR HARM500_G=1

HARM520_FG. [S] Did your next job pay less, the same, or more than the job from which you quit or got fired?

1. Less
2. Same

3. More
4. I did not get another job after quitting or getting fired **[SEPARATE BY ½ LINE FROM OPTION 3]**

BASE: HARM520_FG=1 OR 3

HARM530_FG. [S] [IF HARM520_FG=1, INSERT: About how much less money did you make per month?**] [IF HARM520_FG=3, INSERT**: About how much more money did you make per month?**]**

1. $0
2. $1 to $100
3. $101 to $500
4. $501 to $1,000
5. $1,001 to $5,000
6. $5,001 or more
7. Don't know

BASE: HARM530_FG=1, 2, 3, 4, 5, OR 6

HARM540_FG. [S] Was your answer to the previous question estimated based on…?

1. Gross pay <u>before</u> taxes and deductions
2. Take home pay <u>after</u> taxes and deductions

BASE: HARM500_H=1 OR HARM500_I=1

HARM510_HI. [S] Compared to your job at the time, how much more money do you think you would have made per month if you got promoted or got the new job?

1. My monthly pay would have been less
2. $0
3. $1 to $100
4. $101 to $500
5. $501 to $1,000
6. $1,001 to $5,000
7. $5,001 or more
8. Don't know

BASE: HARM510_HI=2, 3, 4, 5, 6, OR 7

HARM520_HI. [S] Was your answer to the previous question estimated based on…?

1. Gross pay <u>before</u> taxes and deductions
2. Take home pay <u>after</u> taxes and deductions

BASE: DOV_ABUSE=1

HARM600 (Other Financial Costs). [BANKED] Did the following happen to you because of the [INSERT DOV_ABUSE_TYPE] you experienced?

Statements:
    A. I took out loans
    B. I spent savings or sold assets
    C. I paid for a credit monitoring or credit repair service
    D. I paid for a personal information removal service
    E. I paid for an image monitoring or removal service
    F. I paid for a lawyer, legal assistance, or legal fees

Responses:
    1. Yes
    2. No

BASE: HARM600_A=1

HARM610_A. [S] About how much money did you take out in loans?

    1. $0
    2. $1 to $500
    3. $501 to $1,000
    4. $1,001 to $5,000
    5. $5,001 to $10,000
    6. $10,001 to $50,000
    7. $50,001 or more
    8. Don't know

BASE: HARM600_B=1

HARM610_B. [S] About how much of your savings or money from assets did you spend?

    1. $0
    2. $1 to $500
    3. $501 to $1,000
    4. $1,001 to $5,000
    5. $5,001 to $10,000
    6. $10,001 to $50,000
    7. $50,001 or more
    8. Don't know

BASE: HARM600_C=1 OR HARM600_D=1 OR HARM600_E=1

HARM610_CDE. [S] About how much did you spend on services to monitor your credit, personal information, or images?

    1. $0
    2. $1 to $500

3. $501 to $1,000
4. $1,001 to $5,000
5. $5,001 to $10,000
6. $10,001 to $50,000
7. $50,001 or more
8. Don't know

HARM610_F. [S] About how much did you spend on lawyers, legal assistance, or legal fees?

1. $0
2. $1 to $500
3. $501 to $1,000
4. $1,001 to $5,000
5. $5,001 to $10,000
6. $10,001 to $50,000
7. $50,001 or more
8. Don't know

HARM700. [S] About how many hours did you spend trying to fix problems related to the [INSERT DOV_ABUSE_TYPE] you experienced, either on your own or with help (such as with lawyers, law enforcement, healthcare professionals, or services)?

1. Less than 1 hour
2. Less than 8 hours
3. About 8 hours
4. More than 8 hours

HARM710. [N] About how many total hours would you guess that you spent trying to fix problems related to the [INSERT DOV_ABUSE_TYPE] you experienced?

[NUMERIC BOX, RANGE: 0 TO 999] hours

PROGRAMMER: Please add the below text under the next button in smaller font (-1 font size) on the same screen as HARM710.

If you need help or are experiencing distress, please contact the National Domestic Violence Hotline at 1-800-799-7233 or online.

DISCRETE CHOICE EXPERIMENT SECTION for WILLINGNESS-TO-PAY COST ESTIMATION

BASE: ALL RESPONDENTS

DC_INTRO. [DISPLAY]

Now we're going to ask your opinions about some ways to reduce these abuses. Some programs can reduce the number of people affected by image-based sexual abuse, doxing, and cyberstalking as well as reduce how much harm is caused to victims. These programs can include

- Providing financial and technical assistance and therapy to help victims deal with the consequences
- Providing modern technology to help victims monitor and delete content or block users
- Public awareness campaigns
- More police enforcement and longer sentences for offenders

In this next section, we are interested in how much you would be willing to actually pay per year for these types of programs.

BASE: ALL RESPONDENTS

DOV_DC_IBSA1. [HIDDEN VARIABLE – RANDOMLY ASSIGN 1 VALUE]

1. $1,000
2. $500
3. $250
4. $100

BASE: ALL RESPONDENTS

DOV_DC_IBSA2. [HIDDEN VARIABLE – RANDOMLY ASSIGN 1 VALUE, VALUE MUST BE LESS THAN VALUE ASSIGNED AT DOV_DC_IBSA1]

1. $500
2. $250
3. $100
4. $50

PROGRAMMER: Place DC_IBSA_INTRO, DC_IBSA100, DC_IBSA110, and DC_IBSA120 on the same screen.

BASE: ALL RESPONDENTS

DC_IBSA_INTRO. [DISPLAY]

As defined before, **image-based sexual abuse (IBSA)** includes acts such as <u>threatening to disseminate</u> a partially nude, nude, or sexually explicit image or <u>actually disseminating</u> that image, without the consent of the person depicted.

- About 2,400 out of every 100,000 U.S. adults (2.4%) have experienced IBSA in the past

year.

- People who experience IBSA often have psychological distress, fear that they might be recognized by someone they know, relationship difficulties, and reputation damage. Sometimes they also experience job loss, having to leave school, or other severe consequences.

BASE: ALL RESPONDENTS

DC_IBSA100. [S] There are a number of programs that could be considered to reduce IBSA. Which of these programs would you be willing to actually pay for each year?

1. Program A cuts IBSA from 2,400 to 1,200 per 100,000 adults (a 50% decrease). This program would cost your household [INSERT VALUE SELECTED AT DOV_DC_IBSA1] per year.
2. Program B cuts IBSA from 2,400 to 1,800 per 100,000 adults (a 25% decrease). This program would cost your household [INSERT VALUE SELECTED AT DOV_DC_IBSA2] per year.
3. Do nothing – IBSA would remain at 2,400 per 100,000 adults. This would cost your household $0 per year.

BASE: ALL RESPONDENTS

DC_IBSA110. [T] Why did you choose that option?

[TEXT BOX FOR 512 CHARACTERS]

BASE: ALL RESPONDENTS

DC_IBSA120. [S] How certain are you about the option you chose?

1. Very uncertain
2. Somewhat uncertain
3. Somewhat certain
4. Very certain

BASE: ALL RESPONDENTS

DOV_DC_DOX1. [HIDDEN VARIABLE – RANDOMLY ASSIGN 1 VALUE]

1. $1,000
2. $500
3. $250
4. $100

BASE: ALL RESPONDENTS

DOV_DC_DOX2. [HIDDEN VARIABLE – RANDOMLY ASSIGN 1 VALUE, VALUE MUST BE LESS THAN VALUE ASSIGNED AT DOV_DC_DOX1]

1. $500

2. $250
3. $100
4. $50

PROGRAMMER: Place DC_DOX_INTRO, DC_DOX100, DC_DOX110, and DC_DOX120 on the same screen.

DC_DOX_INTRO. [DISPLAY]

As defined before, **doxing** is when someone releases your personal contact or other sensitive information to others without your consent.

- About 1,600 out of every 100,000 U.S. adults (1.6%) have experienced doxing in the past year.
- People who experience doxing often deal with harassing posts and messages from many people, psychological distress, and expenses associated with removing their online information. Sometimes they also experience reputation damage, relationship difficulties, needing to change phone numbers, and even having to move somewhere new.

DC_DOX100. [S] There are a number of programs that could be considered to reduce doxing. Which of these programs would you be willing to actually pay for each year?

1. Program A cuts doxing from 1,600 to 800 per 100,000 adults (a 50% decrease). This program would cost your household [INSERT VALUE SELECTED AT DOV_DC_DOX1] per year.
2. Program B cuts doxing from 1,600 to 1,200 per 100,000 adults (a 25% decrease). This program would cost your household [INSERT VALUE SELECTED AT DOV_DC_DOX2] per year.
3. Do nothing – doxing would remain at 1,600 per 100,000 adults. This would cost your household $0 per year.

DC_DOX110. [T] Why did you choose that option?

[TEXT BOX FOR 512 CHARACTERS]

DC_DOX120. [S] How certain are you about the option you chose?

1. Very uncertain
2. Somewhat uncertain
3. Somewhat certain
4. Very certain

BASE: ALL RESPONDENTS

DOV_DC_STALK1. [HIDDEN VARIABLE – RANDOMLY ASSIGN 1 VALUE]

1. $1,000
2. $500
3. $250
4. $100

BASE: ALL RESPONDENTS

DOV_DC_STALK2. [HIDDEN VARIABLE – RANDOMLY ASSIGN 1 VALUE, VALUE MUST BE LESS THAN VALUE ASSIGNED AT DOV_DC_STALK1]

1. $500
2. $250
3. $100
4. $50

PROGRAMMER: Place DC_STALK_INTRO, DC_STALK100, DC_STALK110, and DC_STALK120 on the same screen.

BASE: ALL RESPONDENTS

DC_STALK_INTRO. [DISPLAY]

As defined before, **cyberstalking** is when someone uses technology to repeatedly harass another person, stalk them, or monitor their activity.

- About 3,200 out of every 100,000 U.S. adults (3.2%) have experienced cyberstalking in the past year.
- People who experience cyberstalking often alter their daily routines, feel at risk no matter where they are, feel psychological distress or fear, and have stress-related health problems. They also may have expenses related to closing and opening new accounts, paying for therapy, improving home security, and replacing electronic devices like their phone.

There are a number of programs that could be considered to reduce cyberstalking. Which of these programs would you be willing to actually pay for each year?

1. Program A cuts cyberstalking from 3,200 to 1,600 per 100,000 adults (a 50% decrease). This program would cost your household [INSERT VALUE SELECTED AT DOV_DC_STALK1] per year.
2. Program B cuts cyberstalking from 3,200 to 2,400 per 100,000 adults (a 25% decrease). This program would cost your household [INSERT VALUE SELECTED AT DOV_DC_STALK2] per year.
3. Do nothing – cyberstalking would remain at 3,200 per 100,000 adults. This would cost your household $0 per year.

DC_STALK100. [S]

DC_STALK110. [T] Why did you choose that option?

[TEXT BOX FOR 512 CHARACTERS]

DC_STALK120. [S] How certain are you about the option you chose?

1. Very uncertain
2. Somewhat uncertain
3. Somewhat certain
4. Very certain

COST100. [S] Who do you believe should pay for programs to prevent image-based sexual abuse, doxing, and cyberstalking?

PROGRAMMER: Randomize statements 1-2
1. Government – paid for by taxes
2. Tech companies – paid for by customers or by having to see more ads
3. Other, please describe: **[TEXTBOX, ANCHOR]**

COST110. [N] Suppose your mayor was given $1,000 per household to spend on programs to reduce image-based sexual abuse, doxing, and cyberstalking in your community.

Out of $1,000, how much would you spend on each program below? You can spend all of it on one program or split it up in any way you want, but the total should add up to $1,000.

PROGRAMMER: Show a column of numeric boxes next to each statement with a range of 0 to 1000. Constant sum indicator should indicate remainder of the $1,000 under the column of numeric boxes.
PROGRAMMER: Randomize statements 1-6
1. Prevention programs to educate people that these behaviors are crimes
2. Education on how to protect oneself from these crimes
3. Tougher punishment for people who commit the crimes
4. More secure technology to prevent these crimes from happening
5. More secure technology to help victims monitor and delete online material
6. Victim assistance programs that provide compensation, therapy, and other services
7. Share the money with all households in the community through a tax rebate **[ANCHOR]**

IDEO100. [S] In general, how do you see yourself?

1. Very liberal

2. Liberal
3. Slightly liberal
4. Moderate
5. Slightly conservative
6. Conservative
7. Very conservative

BASE: ALL RESPONDENTS

IDEO110. [S] How do you see yourself on **social issues**?

1. Very liberal
2. Liberal
3. Slightly liberal
4. Moderate
5. Slightly conservative
6. Conservative
7. Very conservative

BASE: ALL RESPONDENTS

IDEO120. [S] How do you see yourself on **economic issues**?

1. Very liberal
2. Liberal
3. Slightly liberal
4. Moderate
5. Slightly conservative
6. Conservative
7. Very conservative

BASE: ALL RESPONDENTS

IDEO130. [S] In general, do you believe taxes are…?

1. Too low
2. About right
3. Too high

BASE: XHEALTH1=2

Health1 [M]

Have YOU been diagnosed by a doctor or other qualified medical professional with any of the following mental health conditions? Select all answers that apply.

1. Anxiety disorder
2. Depression
3. Mood disorder
4. Post-traumatic stress disorder (PTSD)
5. None of these **[S]**

CU3 [S]

Do you regularly check or post on social media on a smartphone, tablet, or other mobile device?

1. Yes, regularly do

2. No, do not regularly do

CU1 [S]

How concerned are you about providing personal information over the internet?

 1. Not at all concerned

2. Slightly concerned

3. Somewhat concerned

4. Very concerned

PA3 [S]

What sex were you assigned at birth on your original birth certificate?

1. Male

2. Female

PA1 [MP]

What is your current gender identity? Select all answers that apply.

1. Male

2. Female

3. Transgender

4. Non-binary

5. A different identity, please specify [O]

PA2 [S]

Which of the following best describes how you think of yourself?

1. Gay or lesbian

2. Straight, that is, not gay

3. Bisexual

4. Something else

ppcp0005 [Q]

In a typical week, about how many hours do you spend on the internet for personal use? If none, enter "0". If less than an hour in a week, enter "1".

Type in the number for the answer

SCRIPTER: Show one box labeled "hours spent on the internet for personal use in a typical week" min.=0, max.=168; do not allow decimals.

QF1. [T] Thank you for taking our survey! Do you have any comments about this survey?

      [TEXT BOX FOR 2048 CHARACTERS]

HELP_SCREEN. [DISPLAY] If you need help or are experiencing distress, please contact the National Domestic Violence Hotline at 1-800-799-7233 or online.

END OF QUESTIONNAIRE

Appendix 2: SME Interview Instrument

Oral Interview Informed Consent Form

Hi, my name is _____, and I'm with the Justice Research and Statistics Association. Thank you for agreeing to speak with me today. We here at JRSA have asked to interview you based on your knowledge and experience in the area of technology facilitated abuse. This interview is taking place as part of a research project funded by the National Institute of Justice. Our main research objective is to develop a complete map, or taxonomy, of consequences suffered by victims of cyberstalking, nonconsensual or revenge porn, and doxing. In order to gain a full understanding of these consequences, we are conducting interviews with individuals who work in the field of technology facilitated abuse or who are survivors.

If you agree to participate in this interview it should take approximately 60 minutes to complete. All questions are strictly related to your perceptions and opinions on consequences suffered by [victims, you] as a result of victimization and costs (victims, you] or others may have had to pay. [Survivors: We will not be asking any personal or sensitive questions about your victimization experience.] Your participation is completely voluntary, and you can refuse to answer any question or end the interview at any time. Your participation and responses will be kept confidential, meaning we will not share your name in any reports related to this project. However, while comments will not be attributed to you individually, it is possible that others may suspect it is your comment depending on the content. De-identified data from this study that does not include anyone's name or other personal information will be archived with the National Archive of Criminal Justice Data as required by US code 28 CFR §22.23(b)(4). There are no risks to participating in this study. If you are not participating in this interview in your professional capacity (i.e., in your professional capacity and on your employer's time), there is a $50 stipend for participating.

Do you understand that participation is voluntary?

Yes   No   Interviewer's Signature and Date _____

Do you consent to participate?

Yes   No   Interviewer's Signature and Date _____

If you have any questions you can contact me by phone or email. If you have any questions about your rights as a human subject in a research study, please contact Dr. Kris Lugo-Graulich (202.842.9330), who is JRSA's IRB officer.

I have discussed the proposed research with this participant, and in my opinion, the participant understands the benefits, risks, and alternatives (including non-participation) and is capable of freely consenting to participate in the research.

Signature _____ Date _____

Name (Printed) _____

SME/Survivor-Advocate Interview Questions

(To be customized for each interviewee based on background. Several of these questions ask about interviewees' impressions or ideas that can inform our national survey.)

We are asking today about three specific types of technology-facilitated abuse: cyberstalking, nonconsensual pornography ("revenge porn"), and doxing—specifically within an intimate partner context. For these purposes, we would classify any abuse with a technology component to it as technology facilitated abuse, even if the technology is simply a tool being used in a larger pattern of activity. We also realize that incidents may more than one of type of technology-facilitated abuse at the same time. Cased on initial information about your background, it appears you have experience with _____. Is this correct?

Definitions of the Crime

First, I want to ask you some questions about how you would define these crimes and how common they are. Later, I will ask you more specific questions about the harm caused by as well as society's response to each type of crime.

1. These are relatively new crimes over the last couple of decades, and they are continually evolving., I'd like to read you a definition for _____ that was recently published and ask you whether you think it's accurate, or what you would change about it. As a reminder, this study is examining these crimes when perpetrated within an intimate partner context.
   a. Cyberstalking, generally, is repeated use of electronic communications to stalk a person.
   b. Doxing: one definition of doxing is when an individual's personal contact or other information is published on the internet or otherwise distributed to others via electronic means without their consent.
   c. Nonconsensual pornography is when nude or sexually explicit images are distributed without one's consent, and is considered by some to be a form of doxing while others have defined it as a separate crime.

2. More broadly, how would you define an intimate partner in these circumstances? How well does the individual need to know the perpetrator to include their victimization in that category?

3. Based on your expertise in _____, how common is _____, to your knowledge?

    a. Do you see it being more common with one demographic group than another? Is there something that makes their risk level higher in your opinion?

    b. Do you see technology-facilitated abuse as part of a larger pattern of abuse that also occurs in-person? What abuses often co-occur?

4. What other types of technology-facilitated abuse do you think are important to consider in the intimate partner context? Why? How would you define that/those?

5. What should we know about the methods or tactics of how these crimes are committed that could impact how they are addressed in law, policy, or by those providing services?

6. Are there particular aspects of these crimes that are different because they take place over technology, as opposed to their offline counterparts such as in-person stalking or harassment?

    a. For example, does the online environment impact the nature or speed of escalation of these forms of harassment and intimidation? How does it impact the experiences of the victim?

Harms and Consequences of Technology-Facilitated Abuse in an Intimate Partner Context

Now, I'd like to focus on the consequences and victim harm from these crimes.

7. Can you please describe the types of harms and costs you have seen to victims as a result of these crimes? Costs could be considered in dollars, but also in time spent, trauma experienced, and so on.

    <u>Prompts if needed:</u>

    a. Safety
    b. Mental Health
    c. Reputation
    d. Physical Health
    e. Educational Attainment
    f. Legal system
    g. Financial
    h. Removing content, repairing stolen identities, repairing credit
    i. Harms to Society
    j. What other ones can you think of?

    [Interject as needed to ask for more description of each. We can ask individuals to rank them in severity when we get to the Advisory Board meetings.]

8. Do you see *differences in the frequency or severity of these harms* when the abuse is technology-facilitated only, in-person only, or both? Please describe.

     a. Do you see these experiences vary by different demographic groups?

9. Which of these harms are lingering harms that individuals must deal with for an extended period of time? I am not talking about lingering/ongoing abuse. Instead, one example of a lingering harm might be the reputational effects of delays in getting pictures or personal information taken down. You may have others to talk about.
     a. What do you think makes them so difficult to deal with?

10. Do any of these consequences you mention lead to other problems as well? How so? Please describe.

Help Seeking and Barriers to Help Seeking

Next, I want to ask you some questions about victim assistance.

11. What kinds of assistance do you think would be of most help for victims of_____? Why?
     a. Do you think these are adequately supplied or available to victims? If not, why not?

12. What would you like others to know about helping victims of ____, especially in the intimate partner context?

13. Do you think that victims of _____ can become stigmatized by others?
     a. Are there particular types of stigma associated with this type of victimization? How so?
     b. What harms do you think are caused by this stigma?
     c. Do you think this prevent people from seeking help? How so?
     d. Do you think this happens differently with different demographic groups? How so?

14. To your knowledge, are victims of these crimes likely to report to police? Why or why not?

15. Are there particular demographic groups more likely to disclose this sort of victimization in another setting, like a hospital or with another type of service provider? Why? And how do these patterns vary?

16. What do you think is the most important thing you have seen victims do to help themselves after they were victimized?
     a. What key strategies do you see survivors using? What are your thoughts about these?

For National Survey

Finally…

17. Our next steps in this research are to have some group discussions with our Advisory Panel as we prepare to conduct a national survey. This survey will be used to generate some estimates about the prevalence of cyberstalking, nonconsensual pornography, and doxing in the intimate partner context, as well as to generate information to estimate the costs associated with these crimes to victims and to society. We'd like to ask you three questions that would help us with that survey:
    a. If you could ask one question in this national survey, what would that be?
    b. What is the most important information, in your opinion, that could come from a national survey?
    c. Are there any pitfalls you foresee or cautions you'd offer in developing the national survey?

18. What else do you wish people knew about technology-facilitated abuse that we have not covered?

Thank you! We appreciate your help with this important research.

Appendix 3: KnowledgePanel Survey Methodology

KnowledgePanel Methodology

KnowledgePanel provides probability-based samples with an "organic" representation of the study population for measurement of public opinions, attitudes, and behaviors. The panel was first developed in 1999 by Knowledge Networks, an Ipsos company. Panel members are randomly selected so that survey results can properly represent the U.S. population with a measurable level of accuracy and a calculable response rate, features that are not obtainable from nonprobability or opt-in online panels (for comparisons of results from probability versus nonprobability methods, see MacInnis et al., 2018[16] and Yeager et al., 2011[17]).

KnowledgePanel's recruitment process was originally based exclusively on a national RDD sampling methodology. In 2009, in light of the growing proportion of cellphone-only households, Ipsos migrated to an ABS recruitment methodology via the U.S. Postal Service's Delivery Sequence File (DSF)[18]. ABS not only improves population coverage, but also provides a more effective means for recruiting hard-to-reach individuals, such as cellphone-only households, non-internet households, young adults, and persons of color. Households without an internet connection are provided with a web-enabled device and free internet service.

After initially accepting the invitation to join the panel, participants are asked to complete a short demographic survey (the initial Core Profile Survey); answers to this survey allow efficient panel sampling and weighting for future surveys. Upon completing the Core Profile Survey, participants become active panel members. All panel members are provided privacy and confidentiality protections.

Adults from sampled households are invited to join KnowledgePanel through a series of mailings, including an initial invitation letter, a reminder postcard, and a subsequent follow-up letter. Moreover, telephone refusal-conversion calls are made to nonresponding households for which a telephone number could be matched to a physical address. Invited households can join the panel by:

- Completing and mailing back a paper form in a postage-paid envelope
- Calling a toll-free hotline phone number maintained by Ipsos
- Going to a designated Ipsos website and completing the recruitment form online

KnowledgePanel Latino Recruitment

In 2008, KnowledgePanel Latino[SM] was developed to provide researchers with the capability to conduct representative online surveys with United States Hispanics, including both English and Spanish-dominant Hispanics. With the advent of KnowledgePanel Latino, the first United States online panel representative of Hispanics was established to include those without Internet access and those who only speak Spanish. Hispanic members recruited through our traditional ABS sampling methodology described above are supplemented with recruitment using a custom dual-frame RDD sampling methodology targeting telephone exchanges associated with census blocks that have a 65% or greater Latino population density

---

[16] MacInnis, B., Krosnick, J., Ho, A., and M. Cho (2018). "The Accuracy of Measurements with Probability and Nonprobability Survey Samples: Replication and Extension." Public Opinion Quarterly, Winter 2018.

[17] Yeager, D., Krosnick, J., Chang, L., Javitz, H., Levendusky, M., Simper, A. and R. Wang (2011). "Comparing the Accuracy of RDD Telephone Surveys and Internet Surveys Conducted With Probability and Non-Probability Samples." Public Opinion Quarterly, Winter 2011.

[18] Fahimi, M. and D. Kulp (2009). "Address-Based Sampling – Alternatives for Surveys That Require Contacts with Representative Samples of Households." Quirk's Marketing Research Review, May 2009.

(this density level covers just over 50% of the United States Hispanic population). Moreover, cellular numbers from rates centers with high concentration of Hispanics are also used to improve the representation of samples. With this telephone recruitment, households are screened in the Spanish language to only recruit those homes where Spanish is spoken at least half the time.

Household Member Recruitment

During the initial recruitment survey, all household members are enumerated. Following enumeration, attempts are made to recruit every household member who is at least 13 years old to participate in KnowledgePanel surveys. For household members aged 13 to 17, consent is collected from the parents or the legal guardian during the initial recruitment interview. No direct communication with teenagers is attempted before obtaining parental consent.

Survey Sampling from KnowledgePanel

Once panel members are recruited and profiled by completing our Core Profile Survey, they become eligible for selection for client surveys. Typically, specific survey samples are based on an equal probability selection method (EPSEM) for general population surveys. Customized stratified random sampling based on "profile" data can also be implemented as required by the study design. Profile data can also be used when a survey calls for pre-screening—that is, members are drawn from a subsample of the panel, such as females, Republicans, grocery shoppers, etc. (This can reduce screening costs, particularly for lower incidence subgroups.) In such cases, we ensure that all subsequent survey samples drawn that week are selected in such a way as to result in a sample that remains representative of the population distributions.

As detailed above, significant resources and infrastructure are devoted to the recruitment process for KnowledgePanel so that our active panel members can properly represent the adult population of the U.S. This representation is achieved not only with respect to a broad set of geodemographic indicators, but also for hard-to-reach adults (such as those without Internet access or Spanish-language-dominant Hispanics) who are recruited in proper proportions. Consequently, the raw distribution of KnowledgePanel mirrors that of the U.S. adults fairly closely, barring occasional disparities that emerge for certain subgroups due to differential recruitment and attrition.

For selection of general population samples from KnowledgePanel, a patented methodology has been developed such that samples from the panel behave as EPSEM samples. Briefly, this methodology starts by weighting the pool of active members to the geodemographic benchmarks secured from a combination of the U.S. Census Bureau's American Community Survey (ACS) and the latest March supplement of the U.S. Census Bureau's Current Population Survey (CPS) along several dimensions. Typically, the geodemographic dimensions used for weighting the entire KnowledgePanel include the following dimensions, with additional nesting of dimensions as well:
- Gender (Male/Female)
- Age (18–29, 30–44, 45–59, and 60+)
- Race/Hispanic ethnicity (White/Non-Hispanic, Black/Non-Hispanic, Other or 2+ Races/Non-Hispanic, Hispanic)
- Education (Less than High School, High School, Some College, Bachelor and beyond)
- Census Region (Northeast, Midwest, South, West)
- Household income (under $10k, $10K to <$25k, $25K to <$50k, $50K to <$75k, $75K to <$100k, $100K to <$150k, and $150K+)
- Home ownership status (Own, Rent/Other)
- Household size (1, 2, 3, 4+)

Technology-Facilitated Abuse in Intimate Partner Violence (IPV): An Exploration of Costs and Consequences: Final Report

- Metropolitan Area (Yes, No)
- Hispanic Origin (Mexican, Puerto Rican, Cuban, Other, Non-Hispanic)
- Language Dominance (non-Hispanic and English Dominant, Bilingual, and Spanish Dominant Hispanic) when survey is administered in both English and Spanish

Using the resulting weights as measures of size, a probability-proportional-to-size (PPS) procedure is used to select study specific samples. It is the application of this PPS methodology with the imposed size measures that produces demographically balanced and representative samples that behave as EPSEM. Moreover, in instances where a study design requires any form of oversampling of certain subgroups, such departures from an EPSEM design are accounted for by adjusting the design weights in reference to the Census benchmarks for the population of interest.

Survey Administration
Once assigned to a survey, members receive a notification email letting them know there is a new survey available for them to complete. This email notification contains a link that sends them to the survey. No login name or password is required. The field period depends on the client's needs and can range anywhere from a few hours to several weeks.

Typically, after three days, automatic email reminders are sent to all non-responding panel members in the sample. Additional email reminders are sent and custom reminder schedules are set up as needed. To assist panel members with their survey taking, each individual has a personalized member portal listing all assigned surveys that have yet to be completed.

Ipsos also operates an ongoing modest incentive program to encourage participation and create member loyalty. The incentive program includes special raffles and sweepstakes with both cash rewards and other prizes to be won. On average, panel members complete three to four surveys per month with durations of about 10 to 15 minutes per survey. An additional incentive is usually provided for longer surveys.

Response Rates
As a member of the American Association of Public Opinion Research (AAPOR), Ipsos follows the AAPOR standards for response rate reporting. While the AAPOR standards were established for single survey administrations and not for multi-stage panel surveys, we use the Callegaro-DiSogra (2008)4 algorithms for calculating KnowledgePanel survey response rates.

Ipsos KnowledgePanel Weighting

Study-Specific Post-Stratification Weights
Once all survey data have been collected and processed, design weights are adjusted to account for any differential nonresponse that may have occurred. Depending on the specific target population for a given study, geodemographic distributions for the corresponding population are obtained from the CPS, the U.S. Census Bureau's American Community Survey (ACS), or in certain instances from the weighted KnowledgePanel profile data. For this purpose, an iterative proportional fitting (raking) procedure is used to produce the final weights. In the final step, calculated weights are examined to identify and, if necessary, trim outliers at the extreme upper and lower tails of the weight distribution. The resulting weights are then scaled to aggregate to the total sample size of all eligible respondents.

Step 1: Design weights for all KnowledgePanel (KP) assignees were computed to reflect their selection probabilities.

Step 2: The above design weights for KP respondents were raked to the following geodemographic distributions of the 18 and over US population. The needed benchmarks were obtained from the 2022 March Supplement of the Current Population Survey (CPS), except for language proficiency within Hispanics, the benchmarks were obtained from the 2021 American Community Survey (ACS).

- Gender (Male and Female) by Age (18-29, 30-44, 45-59, 60+)
- Race-Ethnicity (White/Non-Hispanic, Black/Non-Hispanic, Other/Non-Hispanic, Hispanic, 2+ Races/Non-Hispanic)
- Census Region (Northeast, Midwest, South, West) by Metropolitan Status (Metro, Non-Metro)
- Education (Less than High School, High School, Some College, Bachelor or higher)
- Household Income (under $25K, $25K-$49,999, $50K-$74,999, $75K-$99,999, $100K-$149,999, $150K and over)
- Language Dominance (English Dominant Hispanic, Bilingual Hispanic, Spanish Dominant Hispanic, Non-Hispanic)

The resulting weights were scaled to add up to the sample size of respondents and were labeled as ***weight*** with 2,521 cases.

Trimming: None
Design Effect: 1.0904