

TECC Whitepaper Series, 2019

Gender-Based Violence and Technology-Enabled Coercive Control in Seattle:

Challenges & Opportunities



by Dana Cuomo, PhD & Natalie Dolci, LICSW

Table of Contents

Acknowledgements	3
Introduction & Overview of the Problem	4
Project Objectives	5
Methodology & Methods	6
Summary Findings & Recommendations	8
Establishing the TECC Landscape	12
Findings	18
Finding 1: The Impact of TECC on Survivors is Significant	18
Finding 2: Seattle Lacks a Training & Consultation Structure for Addressing TECC	22
Finding 3: Seattle’s Response to Address TECC is Inconsistent & Inadequate	26
Finding 4: Seattle Lacks Sufficient TECC-Specific Prevention Education and Community-Based Resources	30
Recommendations	34
Recommendation 1: Improve Regional Partnerships and Collaboration	34
Recommendation 2: Increase Consistency of the System Response to TECC	36
Recommendation 3: Implement Standardized & Consistent Training Structures	39
Recommendation 4: Enhance TECC-Specific Prevention Education and Community-Based Resources	41
Recommendation 5: Implement Protection Order Modernization Project	43
Conclusions and Next Steps	46
References	47

Acknowledgements

This research was a collaborative effort, spearheaded by Dana Cuomo, Assistant Professor of Women's and Gender Studies at Lafayette College and Natalie Dolci, City of Seattle. Dana and Natalie together conducted the original research and analysis, but would not have been able to complete the research or this report without the help of many dedicated partners.

We would like to thank members of the Technology-Enabled Coercive Control (TECC) Working Group for their early efforts in drafting a proposal to conduct research on TECC in Seattle. We would also like to thank Dana Lockhart for permitting Natalie to conduct this research while situated in the Seattle Police Department's Victim Support Team, and for facilitating introductions to conduct interviews with numerous agencies and organizations, including the Seattle Police Department Domestic Violence Unit. Thank you especially to all of our research participants who willingly agreed to be interviewed, and who also helped to recruit additional participants to the project.

We would like to thank our incredible research assistants including Amanda Beavin for transcribing interviews and conducting a comprehensive TECC literature review, Julia Borders for transcribing interviews, and Sarah Hall for researching local and national cybercrime laws. We also thank Cate Root for providing report edits and valuable input, and Devin Owens for his creative expertise and transforming this report into its final product.

Dana would like to thank Western Kentucky University for providing financial support to conduct this research (Research and Creative Activities Program Grant #19-8006).

We want to thank advocates for taking time to participate in this project and for the critical work they do every day to support survivors. Most importantly, we would like to extend our gratitude to the survivors of TECC who participated in this project and who shared their experiences with us. Each hoped that by sharing their stories they could contribute to positive change for future survivors.

Introduction & Overview of the Problem

As technology plays an increasingly important role in our everyday lives, it has also become an incredibly effective tool for those who engage in stalking, harassment, and abuse. While scholars and direct service providers refer to this emerging form of abusive behavior through a variety of idioms, in this report we use Technology-Enabled Coercive Control (TECC) to capture the breadth and scope of the problem.

Coercive control reflects a pattern of behavior that is designed to assert influence and control over an individual's life using threats of harm, dependence, isolation, intimidation, and/or physical forms of violence, often resulting in a survivor losing a sense of their self-worth, bodily integrity, and safety (Dutton and Goodman 2005; Stark 2007). TECC extends this pattern of behavior to include the ways technology facilitates coercive control. Forms of TECC include cyberstalking, monitoring, impersonation, harassment, distribution of intimate images, along with other related patterns of violence that use technology as a tool to abuse, harass, and stalk. In the context of intimate partner violence, those who engage in TECC rely on overlapping tactics and evolving forms of technology to instill feelings of fear, isolation, confusion, and terror among those they are targeting.

In establishing the scope of the problem and the context for this report, we draw on over ten years of research that affirms the way TECC represents a central – rather than ancillary - element of abuse (Fraser et al 2010). This includes a National Network to End Domestic Violence (NNEDV) survey that indicates 97% of programs who provide advocacy and support services report that abusers misuse technology to stalk, harass, and control survivors (2014). TECC is not only prevalent and pervasive, it is now standard and often the primary form of abuse that intimate partner violence, sexual assault, and stalking survivors experience.

Those who use technology as a tool to engage in coercive control benefit from its affordability, accessibility, and usability. Most tech-based harassment occurs on social media platforms and phone-based apps, which are free or low-cost. More complex spyware and malware software are available for purchase online and obtained instantly. An overall cultural acceptance of tracking and monitoring as ordinary behavior also aids those who abuse technology. Notably, this normalization ranges from the presence of surveillance cameras in public space, to the development of a suite of products marketed to parents to track and monitor children, to the colloquial practice of “Facebook stalking”. The normalization of technology to surveil in everyday life also serves to minimize its perceived effects on survivors. Additionally, research indicates that most stalkers rely on unsophisticated forms of technology to engage in coercive control (Freed et al 2018), furthering the problematic notion that this misconduct is trivial and inconsequential.

As those who engage in TECC display a persistent capability to evolve and advance in their use of technology to harass and terrorize, the systems meant to support survivors and hold offenders accountable continue to lag behind. This is despite the warning issued nearly fifteen years ago by scholars and those working in the field of gender-based violence that technology represented an emerging and serious form of abuse (Southworth and Tucker 2006). These scholars and advocates cautioned systems to recognize the risk TECC posed for intimate relationships and to institute training and dedicate resources to respond (King-Ries 2010). Today, those who abuse technology maintain the advantage as TECC continues to outpace current laws, despite a recent flurry of newly enacted cybercrimes legislation across the country, particularly in response to nonconsensual pornography and the disclosure of intimate images (McNeal et al 2018; Southworth et al 2007; Dunlap 2012; Goldsworthy et al 2017; Shimizu 2013).

While scholars note recent legislative improvements, they also argue that more needs to be done within and beyond the law (Henry and Powell 2016). Such is the case because even when cybercrime laws exist, research indicates that those working within the civil and criminal legal systems minimize TECC and even treat survivors with scorn (Sweeny 2017). Challenges in supporting survivors extend beyond the legal systems, as TECC has also outpaced system and community-based advocacy services, along with existing resources to address survivors’ tech safety planning needs (Tanczer et al 2018). All the while, research and first-hand accounts affirm that experiencing TECC results in significant negative impact on survivors (Freed et al 2018).

Put succinctly, the ability to engage in TECC is easily available to abusers across socio-economic status, it requires little to no formal training or education to be effective, many of the systems meant to support survivors minimize TECC and/or lack sufficient training and resources to effectively respond. Those who engage in TECC are rarely held accountable for their behavior, and thus survivors experience little in the way of relief as TECC’s terrorizing impact wreaks havoc on all aspects of their lives. Such is the context in which we situate this research project.

Project Objectives

Our goal in conducting this research is to provide a resource for advocates, the civil and criminal legal systems, policy makers, and others in the community to better serve survivors who are experiencing TECC. The findings and recommendations that we cohere in what follows draw directly on the insight and perspectives provided by those who participated in this research project. Thus, the information that we synthesize in this report is a compilation of the expert knowledge, feedback, and recommendations of those most closely connected to the problem, including survivors.

Methodology & Methods

The methodological framework guiding this project is rooted in the principles of Community-Based Participatory Action Research (CBPAR). As a research methodology, CBPAR emphasizes the needs and knowledge of the community being studied, and engages community participants as active members of the project. CBPAR attends to inequities and injustices, encourages community members' power over their own lives, works to prevent exclusion and promote diversity of participation, builds and expands on local partnerships, and supports the action necessary to achieve change (Stoecker 2013). CBPAR also begins by assuming that those who have been most systematically excluded or oppressed carry a specific wisdom about their lives and the structures and fracture points that led to their experiences (Kindon et al 2007). In response, CBPAR centers collaborative knowledge production in which knowledge, analysis and action collectively emerge between researchers and participants across all stages of a project with the goal of achieving social action and change (ibid).

Following the principles of CBPAR, this project was developed in collaboration with the Seattle-based Technology-Enabled Coercive Control (TECC) Working Group. The TECC Working Group is a multi-disciplinary group that aims to build the capacity of providers who respond to survivors of technology-enabled coercive control. The TECC Working Group also seeks to build

bridges between the private technology sector, direct service providers, and the civil and criminal legal systems to more effectively provide relief to cyberstalking survivors. The research objectives, questions, and project design were developed in collaboration and then executed by the two-member research team.

“Research is not an innocent or distant academic exercise but an activity that has something at stake and that occurs in a set of political and social conditions.”

-Linda Tuhiwai Smith 2005, p5

For the purposes of our project, the term “Provider” refers to anyone working with survivors of TECC. This includes community-based advocates, systems-based advocates, police, prosecutors, civil/legal aid attorneys, judicial officers, Title IX investigators, threat assessment personnel, etc. Survivors and Providers who participated in the research project are also referred to as “Stakeholders” and “Participants” throughout the report.


Data collection occurred during seven weeks of field work (summer 2018, winter 2019, spring 2019) culminating in 6 in-depth, open-ended qualitative interviews with survivors of TECC¹ and 50 in-depth, semi-structured qualitative interviews with providers from the following Seattle-based agencies²:

Qualitative research allows the researcher to engage in a deep and detailed examination of a problem. Concerns generally associated with this type of research include validity; the researcher is the primary instrument collecting data within a specific institutional context, meaning the research project is not replicable. As a Seattle-based project with action-oriented goals of identifying local policy, practice, and training recommendations to better serve and support survivors of TECC in Seattle, this project is not intended to be replicated.

Interviews were transcribed and analyzed using axial coding based on recurrent emergent themes. The findings and recommendations herein reflect a synthesis of the perspectives and experiences offered by research participants.

¹Survivors received \$50 gift cards as compensation for participating in an interview.

²The research team relied on snowball sampling and research participant contacts to recruit representatives from Seattle-based provider agencies and units to participate in the project. We made a concerted effort to include as many provider and survivor voices and experiences as possible. As a project with potential to extend into additional phases, we encourage agencies who we contacted, but who were unable to participate due to capacity and/or whose perspectives are not reflected here, to contact us directly if you would like to participate in future projects.



Abused Deaf Women's Advocacy Services
API Chaya
Cyber Civil Rights Legal Project
Judicial Officers
King County Prosecutor's Office
New Beginnings
Organization for Prostitution Survivors
Protection Order Advocacy Program
Salvation Army Domestic Violence Programs
Seattle City Attorney's Office
Seattle Police Department
Sexual Violence Legal Services
TECC Clinic Volunteer Technologists
The Northwest Network
University of Washington Police Department
University of Washington Title IX Office
University of Washington Safe Campus
Washington State Department of Corrections
YWCA Domestic Violence Services

Summary Findings & Recommendations

Summary Findings

As an overview of the information contained within this report, we begin by highlighting our primary findings and recommendations. Each subsequent section of this report provides additional information detailing the following:

Finding 1: The Impact of TECC on Survivors is Significant

From detectives to prosecutors to advocates to survivors themselves, consensus among those who contributed to this research project is that TECC has significant adverse impacts on survivors. Individual survivors report an array of physical, emotional, psychological, and financial insecurities that result from experiencing TECC, that TECC negatively impacts every aspect of their lives, and that the effects of experiencing TECC endure long after the last instance of contact. Research participants describe TECC as psychological torture and that it results in constant feelings of hypervigilance, fear, and uncertainty. Research participants report that TECC elicits a sense among survivors that the abuser's presence is constant, unremitting, omnipresent, and inescapable. Research participants also describe TECC as debilitating and that it causes feelings of hopelessness. For survivors of TECC who seek relief and accountability through the civil and criminal legal systems, research participants indicate that this process is retraumatizing and often ineffectual.

Finding 2: Seattle Lacks a Training & Consultation Structure for Addressing TECC

Providers identified informal consultation and self-teaching as the primary methods by which they gained knowledge about TECC, and that these were both largely self-motivated endeavors and incumbent upon the individual to seek out and acquire. Existing opportunities to receive formal training on TECC are inconsistent and often one-off trainings, without follow up opportunity to develop expertise. Providers identified the training that they received as helpful, but conveyed concern that knowledge gained from stand-alone trainings quickly becomes obsolete. Moreover, those who received training identified attending different training programs, reflecting a haphazard plan for knowledge building. Providers who work within the civil and criminal legal systems indicated training on TECC (and gender-based violence more broadly) as disproportionately deficient, particularly at the first responder level and when compared to training requirements for other crimes. Research participants also cited positive uses of technology, especially in the context of enhancing a survivor's safety plan, yet providers also noted they lacked a structure for learning

and sharing knowledge about this helpful technology. Because units and offices lack institutionalized opportunities for training, as individuals who develop expertise in the area of TECC transition to new positions, their expertise leaves with them. Transition and high turnover in certain units lends to an informal and ad hoc consultation structure that relies on interpersonal relationships for information sharing. Without a plan to institutionally hold and support this knowledge, providers are unable to provide meaningful help to survivors.

Finding 3: Seattle's Response to Address TECC is Inconsistent & inadequate

Building from Finding 2, research participants indicate that Seattle's response to address TECC is inconsistent and inadequate. Again, this problem is not particular to one office or unit, but occurs as a constant across agencies. Overwhelmingly, providers demonstrate commitment to supporting survivors and holding those who engage in TECC accountable, but identified a need for support and resources in order to do so effectively. Both providers and survivors agree that current practices fall short in effectively responding to survivor concerns. Additionally, at the time of this research, Seattle has not fully integrated TECC into its existing domestic violence, sexual assault, and stalking protocols and assessment strategies. While technology is integrated into our communications, relationships, and workflows, providers often discuss and respond to "cyberstalking" as distinct from "stalking". Survivors experiencing TECC and who report to law enforcement describe filing numerous police reports across jurisdiction that law enforcement fail to connect as a pattern of crime or dismiss as noncriminal behavior altogether. The allocation of resources to investigate and prosecute TECC-based crimes, particularly at the misdemeanor level, are insufficient. The civil protection order process is outdated and survivors of TECC are unable to reliably submit digital evidence into the record. The lack of a comprehensive response both fails and retraumatizes survivors of TECC.

Finding 4: Seattle Lacks Sufficient TECC-Specific Prevention Education and Community-Based Resources

The community currently lacks sufficient TECC-specific awareness raising and educational programming to prevent individuals from experiencing TECC and engaging in TECC, including a lack of focus on concepts such as privacy, digital consent, and bystander intervention when digital consent is not respected. Research participants indicated that current prevention efforts do not begin early enough among youth and that technology companies are notably absent from these awareness-raising conversations. Research participants also indicated a dearth of existing community-based resources to support survivors of TECC, particularly low-income survivors. Survivors of TECC lack sufficient access to material resources, such as low-cost or free smartphones to replace compromised devices, as well as consultative resources, such as access to local, trained technology specialists to provide one-on-one consultation and individualized tech safety planning. Research participants also identified a lack of community-based resources for survivors of acquaintance and stranger stalking occurring outside of an intimate relationship.

Summary Recommendations

Recommendation 1: Improve Regional Partnerships and Collaboration

To establish increased communication and collaboration across units, we recommend establishing a robust and institutionalized consultation and resource sharing structure across all entities involved in the response to TECC. While each unit and direct service provider plays a specific role – from advocate to investigator to prosecutor to judicial officer to Department of Corrections officer – all would benefit from increased communication across units to clarify investigative expectations, filing standards, and supervision plans. Providers

also identified interest in establishing a centralized unit responsible for housing and maintaining shared resources related to TECC, including templates and investigative materials that would be stored on a shared resource drive. We recommend drawing on existing expertise in this area and expanding the Special Operations Unit to serve as a designated technical and consultation resource within King County. We also recommend formalizing communication and collaboration between the public and private sectors, including establishing contacts with tech companies for increased cooperation around investigations, and to develop a potential pool of expert witnesses for civil and criminal proceedings.

Recommendation 2: Increase Consistency of the System Response to TECC

To both establish an effective response to TECC and strengthen Seattle's response to coercive control and related harm, we recommend integrating TECC into existing assessment strategies and protocols. Thus, rather than distinguishing between "cyberstalking" and "stalking", these behaviors would be seen as equivalent to and inextricable from one another. For example, if an advocate is developing a safety plan with a survivor, TECC will be continually assessed for and addressed in the safety plan. Similarly, if an officer responds to a complaint involving technology, the officer will consult TECC-responsive protocols and assessment tools to encourage appropriate digital evidence collection and preservation. Research participants regularly referred to such tools as helpful in providing consistency in other crimes, notably the DUI protocol. We also recommend that providers consider survivor impact at every step of the process. Fear is an element of the crime of stalking and thus should be assessed for by those in an investigative role. Similarly, prosecutors, judicial officers, and other decision-makers and fact finders must consider survivor impact - as opposed to only lethality - when determining whether to file charges, allocate resources, or issue a protection order. Experiencing TECC has resulted in survivors losing

their jobs, a sense of safety, and their public reputations; we cannot only frame the system response around physical violence. Research participants also recommended dedicating increased investigative support to TECC-based crimes, especially misdemeanor cases. Finally, the Department of Corrections should create TECC-specific supervision plans for those under post-incarceration DOC supervision for a TECC-related crime. Taken together, the implementation of the above recommendations will create meaningful intervention at every step of the legal process and a triage system that prioritizes cases based on lethality and survivor impact.

Recommendation 3: Implement Standardized & Consistent Training Structures

We recommend implementation of standardized and consistent training for all providers involved in the response to TECC that accommodates the varying sizes, schedules, and cultures of these entities and agencies. In other words, we do not recommend a one-size-fits-all approach to training on TECC, but rather, diverse training platforms and models best suited to providing units with consistent and up to date information. Research participants recommended a range of ideas to fulfill this individualized training structure, including short, pre-recorded introductory level videos for patrol officers to view at roll call that would allow for large quantities of officers to receive training at once, to updating the judge's manual with TECC-specific information, and recruiting attorneys and tech professionals to write bench memos to share with judicial officers. To develop these training structures, we recommend relying on a combination of local expertise for in-person trainings, supplemented by webinars, and other materials provided by national entities. We also recommend the recording of all local, in-person trainings, which can then be uploaded to a shared drive and become part of an archived, comprehensive training curriculum required for new hires and accessible to providers at any time. We recommend that tech safety planning training content be made available to advocates,

along with regular booster training that reflects the ever-changing landscape of TECC.

Recommendation 4: Enhance TECC-specific Prevention Education and Community-Based Resources

To increase community awareness of TECC, and to prevent individuals from experiencing or engaging in TECC, we recommend providers incorporate TECC-specific education and bystander intervention into current prevention programming, curriculum, and campaigns. Specifically, we recommend utilizing a socio-ecological approach that addresses prevention at individual, interpersonal, community, and societal levels. This approach includes youth-focused Digital Consent prevention education that mirrors existing consent programming to prevent sexual assault and relationship violence. Such digital consent prevention programming encourages safe and healthy interactions when texting, using social media, and sharing information and images/videos online. We also recommend a multi-faceted prevention campaign that encourages parents to discuss digital consent with their children. Research participants also identified the responsibility of private sector tech companies to participate (and lead) public awareness raising TECC prevention campaigns. We recommend that information be made available to survivors, and community members broadly, about how to safely maintain their accounts and data. We also recommend dedicating resources to support survivors' material needs, including a compromised device replacement program and in-home surveillance systems for survivors who identify these and other resources as part of their safety plan. We also recommend providing funding to support, institutionalize, and expand TECC clinics throughout Seattle; TECC clinics provide survivors with free, one-on-one consultation with a trained technologist to assist survivors in identifying points of compromise on devices and to develop safety and mitigation plans in response.

Recommendation 5: Implement Protection Order Modernization Project

The insufficiency of King County's Protection Order process - as it relates to TECC - requires its own focus and action. At the time of this research, no accessible system exists to enter digital evidence into the court record and petitioners continue to file by paper. As a means to modernize the entire protection order process, we recommend stakeholders implement an eCourts Civil Protection Order System modeled after other similar existing systems around the country. This system would allow for electronic petition filing, opportunity to consistently upload and submit digital evidence into the record, to conduct remote hearings through live video feeds, and to send automated email and text messages to confirm order service and to provide alerts regarding hearing continuances and modifications. Such advancements could reduce barriers for survivors to participate in the protection order process and can enable them to more completely share their concerns with the court. The inefficiency of the current system is a problem not only for survivors of TECC, but for every King County provider involved in this issue. Modernizing the protection order process also addresses the potential for liability as the current system's inability to consistently receive digital evidence represents a burden for petitioners, particularly for those whose only evidence is digital.

Establishing the TECC Landscape

Before an in-depth discussion of our project's research findings and recommendations, this section will establish the patterns and trends related to TECC that stakeholders discussed as prevalent in Seattle. This Seattle-specific TECC landscape provides the context for many of our findings and recommendations to follow.

When embarking on this project, we surmised that Seattle's reputation as a tech-savvy region would result in instances and patterns of highly sophisticated and complex forms of TECC. Instead, research participants clarified that technology's accessibility and usability has lowered the threshold for abusers to perpetuate harm and that the majority of individuals abusing technology begin with low tech strategies, such as unwanted texting or social media surveillance. While some abusers adapt their tactics to incorporate higher levels of sophistication, the majority initiated their abusive tactics with basic harassing behaviors in which they took no steps to conceal their identity.



Research participants also reflected on the convenience of technology and how this convenience has implications for coercive control dynamics. Namely, technology has made engaging in coercive control easy. When a pattern of stalking might once have required physically pursuing someone, the work of stalking has been automated and, in many aspects, requires less time and effort by the abuser. When a survivor relocates to flee an abuser, technology facilitates not only finding the survivor, but allows an abuser to continue harassing and terrorizing from afar. The convenience of technology facilitates a shield from consequences for those engaging in TECC, particularly when the behavior crosses jurisdictional boundaries.

Four themes of Technology-Enabled Coercive Control emerged from research participant interviews: Surveillance, Multimodal Harassment, Identity Obfuscation, and Distribution of Intimate Images.

Surveillance

Research participants discussed a variety of TECC-specific surveillance, monitoring, and tracking behaviors that involved a spectrum of illicit activity. Some of these location-tracking efforts involved overt tactics, including tagging on social media or utilizing applications that come pre-loaded on the device, such as “Find My Friends”. Research participants also reported examples of more covert efforts, such as abusers who secretly installed location tracking apps onto survivors’ devices or vehicles, along with abusers who relied on products marketed to parents for tracking children. Participants also noted that abusers who purchased technology for their children (tablet, phone, etc.) would enable location tracking applications on their children’s devices as a mechanism to surveil survivors. Research participants also cited Internet of Things (IoT) technology as increasingly common surveillance strategies. IoT technology extends Internet connectivity into physical devices and everyday objects, such as Nest cameras or remotely accessible baby monitors. Notably,

research participants raised confusion about the legality of in-home surveillance in the context of an abusive relationship and when the survivor was unaware they were being monitored, particularly in relation to Washington’s two-party consent laws.

Research participants also highlighted the role of open-source intelligence in enabling a significant amount of surveillance, along with the way these tools lowered the threshold for monitoring. For example, a research participant described an instance of a person engaging in stalking who consistently monitored the survivor’s property records online to see whether or not she moved. Another example involved an abuser who paid a nominal fee to access online background checks to determine the survivor’s address and then sent the survivor a photo to let the survivor know they had discovered where they were living. Children were often impacted by this type of open-source surveillance, too. In one case, a father who had been abusive to his family and was court-restricted from contacting his former partner and their children, would monitor the website of the child’s school. Through the school website, the father learned about the child’s athletics schedule and posted information about the game on his own social media. Research participants noted that this gray area of stalkers posting on their own social media about the survivor, but not contacting them directly, causes survivors to feel terrorized, but that judicial officers and prosecutors rarely consider indirect contact to be violations of no contact and protection orders.

Abusers also target survivors’ email and other online accounts as a means to monitor, surveil, and track. In order to access survivors’ online accounts, some abusers engage in insidious behavior such as downloading spyware or keylogger onto a survivor’s device, but research participants also indicated that abusers would learn the survivor’s password through other means. For example, abusers might require password sharing as a part of a pattern of coercive control, or in other cases, survivors may not have had robust password management

practices, which left their accounts vulnerable. Some of the most devastating examples involved abusers who accessed a survivor's email account and changed all the passwords and account recovery information, thus permanently locking the survivor out of their own account. Through this tactic, abusers then gained access to additional accounts. Research participants explained the long-term repercussions of this form of surveillance, as survivors who became locked out of their online accounts would lose evidence and personal, professional, and financial information.

Multimodal Harassment

Research participants identified multimodal harassment - unwelcome, harassing contact using a variety of platforms - as one of the most common tactics relied upon by those who engage in TECC. When multimodal harassment is in use, survivors often receive simultaneous and repeat contact from text messages, social media, dating apps, email, etc. In these instances, survivors describe being "blasted" with the same message, threat, or demand on multiple platforms, sometimes up to and exceeding hundreds of contacts a day.

The content of the harassing communications varies. Some patterns of harassment operate as campaigns to discredit and humiliate the survivor. Examples include the disclosure of intimate images, the abuser posting false allegations online about the survivor, or attempts to sabotage the survivor professionally. Other abusive tactics involve unwanted and repeated attempts to reestablish the romantic relationship. Research participants also described a pattern in which individuals abusing technology would engage in social engineering online to try to reach the survivor through friends and family. Once successful in identifying the survivor's friends and family, abusers often contact or surveil those individuals on social media. Survivors often attempt to control their own web presence, but their relatives and friends might have very different privacy practices that the abuser exploits. In other cases, technology is used to communicate or initiate a violent plan. Numerous

participants referred to abusers sending images of guns or emojis of guns via social media to threaten survivors. Others abusing technology would attempt to provoke violence against the survivor from a third party. These examples involved posting a rape fantasy ad online or via a dating application with the survivor's identifying information and individuals would show up at the survivor's home attempting to enact the "fantasy."

In addition to the targeted harassment of creating false rape fantasy profiles on dating apps, research participants mentioned dating apps in other contexts as well. Participants referred to sexual assaults facilitated through dating apps. For example, a survivor may have clearly communicated their boundaries and limits prior to meeting, and then been sexually assaulted by the person they met on the app. The person who assaulted them would then send "normalizing" messages via the app to shape the narrative and attempt to make the exchange appear consensual.

Often, the content of the multimodal harassment fluctuates within short periods of time. For example, a survivor might awaken in the morning to discover hundreds of harassing messages from the abuser that began overnight with apologies and requests to reestablish the relationship. Then, over the course of hours (when the survivor was asleep and not responding), the content escalates to direct threats or campaigns to discredit the survivor. Research participants explained the challenges around comprehensively safety planning when abusers engaged in multimodal harassment, as those who utilized this tactic often switched platforms, profiles, or would target survivors in ways that made it difficult for survivors to change contact information without impacting their personal lives or causing damage to their professional careers.

For incarcerated individuals who engage in TECC, research participants noted jail-based communications as a challenging area for survivors. Participants described instances of incarcerated people continuing to perpetuate harm by switching booking arrest numbers or using three way calls to

to contact the survivor in violation of a court order. The introduction of video chatting has also raised new opportunity for harassment and harm. While increased access to video chatting has some obvious benefits, as it enables loved ones to communicate without the time and expense of travel to and from the jail, this technology can also be an opportunity for invasive abuse. At the time of this research, video calls from jail were not recorded, and providers were unaware of an existing video call policy. As a result, providers explained that video chatting is less transparent than jail phone calls, and cited examples of survivors who experienced threats or violations of protection orders during video chats, but because video calls are not recorded, they lacked proof of the violation. Providers also discussed an example of a survivor who was court-ordered to present her child for jail-based video visitation and explained that this technology allowed the abuser access to the survivor's new home, and that this felt like an invasion to the survivor.

Identity Obfuscation

Those abusing technology rely on a variety of tactics to obfuscate their identity and avoid accountability. Some of these tactics include using numerous accounts and devices to contact the survivor. In other instances, abusers relied on spoofing apps to imply that the calls were coming from a variety of different phone numbers. Research participants also noted that some of these spoofing apps have the ability to disguise the caller's voice. Advocates who work with survivors from the deaf community reported that abusers would call the video relay system and impersonate a legitimate or trusted contact in order to obtain information. As the survivor using the video relay system only sees the sign language interpreter - not the caller - the survivor would not automatically be aware of the deception. Participants also referred to more sophisticated abuses of technology, such as abusers who relied on browsers and networks that thwart surveillance, such as Tor, VPN, or international servers.

Some identity obfuscation efforts involved the use of technology to generate an alibi. Participants mentioned cases in which abusers deliberately left their phone at home while violating a protection order or committing an assault in a different location from their phone. Providers conveyed that cell phone records that placed the abuser at home were sometimes treated as more credible evidence than a survivor's first-hand account of abuse. Another provider referred to an instance in which an abuser drove by the survivor's home, in violation of a no-contact order, and when reported, the abuser referred to a fake craigslist job ad (that he created) as justification for driving by the survivor's home. Other providers noted abusers utilizing tactics such as activating "delay send" features on emails so an email would send during a time when the abuser could claim not having access to email, thus cementing an alibi.

Those who engage in TECC also manipulate app-based ridesharing services, such as Lyft and Uber, in attempts to create an alibi. In one case, a provider described an abuser who asked the driver to be dropped off at his ex-girlfriend's home, despite having entered his own home address into the app. The abuser then violated the protection order by breaking into her home. Providers also described situations in which the rideshare driver directed harassing and abusive behavior toward the passenger, including an instance when a driver turned off the app at the survivor's home, refused to let her out of the car and drove around making unwanted sexual advances towards her. Another example of TECC involving rideshare drivers includes a driver who dropped off a passenger, but returned in the middle of the night and tried to enter the passenger's home. The survivor learned of the driver's attempt to enter her home when she reviewed her Nest cam footage the following morning. These examples reaffirm that simple strategies such as leaving one's phone at home, or enabling "delay send" perpetuate significant harm and allow the abuser to avoid detection without any degree of tech sophistication.

Distribution of Intimate Images

In the context of domestic violence, research participants identified the non-consensual distribution of intimate images (DII) as a consistent form of TECC. These images are generated in a variety of ways. They might be generated consensually during positive periods of the relationship. Alternatively, some partners engage in patterns of coercion to encourage the survivor to allow the images to be taken, even if the survivor is uncomfortable or reluctant. In other situations, the individual engaging in TECC obtained the images covertly through hidden cameras, secretly recording webcam communications, or using other forms of surveillance that the survivor was not aware of at the time. When survivors are unaware that abusers photographed or recorded them, abusers often later used these images or videos to perpetuate patterns of coercive control.

The individual engaging in TECC may use the threat of distributing the intimate images to force someone to remain or return to the romantic relationship, or release the images after the survivor leaves the romantic relationship. Participants reported that in these cases, the distribution of intimate images is one tactic in a broader pattern of power and control. Providers identified the distribution (or threat to distribute) intimate images as additionally damaging in specific cultural contexts, including when survivors fear the shame that this might bring upon themselves and their families. Providers also highlighted how multiple and overlapping oppressive systems create additional impacts for survivors. For example, queer and trans survivors are more likely to experience employment discrimination and Providers indicated that those who threaten to distribute intimate images target survivors' workplaces.

The distribution of intimate images is not confined to intimate relationships. Participants reported other scenarios such as the filming of sexual assaults, the use of non-consensual intimate images within the sex trades, and other financially motivated incidents within and beyond sexual exploitation.

Participants reported that in the context of the sex trades, survivors seeking to exit the life have found it extremely difficult to successfully remove their images from websites advertising them. Those with lived experience in the sex trades also identified the threat of distributing intimate images as a tactic that traffickers and other third-party profiteers use to keep survivors tethered to the life. Those survivors also discussed instances in which buyers paid them to pose naked and the buyers retained the photos. Research participants also noted practices of financial profiteering from intimate images, including examples of unsuspecting individuals who engaged in online chatting that evolved to flirtatious camming in which intimate videos and images were exchanged. After the unsuspecting individual provided intimate images of themselves, the other party threatened to distribute the images unless the unsuspecting individual paid money. This practice has become colloquially known as "sextortion".

Identity obfuscation adds another layer of difficulty to the already devastating situations in which a survivor's intimate images are distributed without their permission. Survivors mentioned tactics such as abusers creating fake Facebook accounts and sending intimate images of the survivor to the survivor's new partner in order to humiliate and continue to assert control. Research participants identified both the threat to and the distribution of intimate images as emotionally damaging, and also extremely easy to perpetrate. Numerous participants reported how technology lowers the threshold for this hurtful behavior and indicated that this level of harm would likely never have occurred via analogue methods.

Regardless of how the images came to be distributed, participants identified how troll communities perpetuate the abuse. In the context of DII, troll communities include individuals who frequent sites dedicated to “revenge porn” and who have no direct tie to the survivor. They take it upon themselves to continue spreading and sharing the intimate images on similar sites. Trolling behavior speaks to the challenges around containment and unmasking, because once strangers and individuals unconnected to the survivor start perpetuating harm, the survivor may have no recourse for pursuing accountability. The ease of transmitting harm minimizes consequences for the abuser, maximizes negative consequences for the survivor, and can serve to further isolate the survivor.

“It’s at your fingertips...He wouldn’t take the time to sit down and write 25 letters. He wouldn’t make those efforts. He wouldn’t write them, and mail them, and buy stamps for them. Because if they didn’t have a smartphone, would they have gone to the library or even gone to the next room to log into their computer? Probably not.”

Advocate

Findings

A detailed review of the research project's primary findings

Finding 1: The Impact of TECC on Survivors is Significant

Research participants affirm that experiencing TECC has significant, deleterious impacts on nearly every aspect of a survivor's life. Here, we discuss four adverse impacts of TECC that research participants highlighted as distinct themes:

TECC Causes Adverse Emotional Impacts

Survivors identified numerous adverse emotional impacts as a result of experiencing TECC. Survivors disclosed feeling constant hypervigilance and fear. This constant fear in part results from abusers who create and capitalize on the perception that they are omnipresent. Participants described abusers who used technology to suggest that they were always watching the survivor and knew the survivor's whereabouts. Regardless of the abuser's locational proximity to the survivor or whether the abuser in fact knew the survivor's location, TECC facilitates the abuser invading the consciousness of the survivor. Abusers may use surveillance to suggest that they are physically close to the survivor, and the survivor might believe that physical violence is imminent. Survivors equate this to a form of emotional terror and psychological torture. Numerous research participants also described physical stalking or physical violence as less terrifying than TECC. These survivors described physical stalking and physical violence as bounded within a specific time and place, while TECC was constant, unrelenting, and inescapable.

Survivors indicate that the constant presence of TECC and the sense that it will never end causes feelings of hopelessness and despair.

Research participants also described the way experiencing TECC contributes to feelings of isolation, especially when a survivor's safety plan included limiting the use of technology. For example, participants reported discontinuing use of Wi-Fi, repeatedly changing their phone number, and even changing the name of their business. While these tech safety planning strategies might result in some (temporary) relief, they often served to further isolate survivors from family, friends, and community. Coercive control relies on isolation of the survivor, and by introducing more isolation into their safety plan, they are by definition, less safe. Research participants also highlighted how the isolating impacts of trying to mitigate TECC affected people with disabilities. For example, advocates who work with deaf survivors noted the role of technology in helping deaf survivors stay socially connected and when abusers compromised deaf survivors' technology, they felt cut off from the world. Research participants also described the impact of receiving

unrelenting blocked and spoofed calls, noting that some survivors became so frightened and fatigued by these calls that they were afraid to go outside or to work. A research participant described working with a survivor who stopped answering the phone or responding to calls, because the survivor feared hearing the abuser's voice. In this example, the survivor's strategy for avoiding her abuser (by not answering her phone) isolated her from those attempting to contact her to provide support and assistance, including advocates, detectives, and attorneys.

In addition to the destabilizing impacts and chronic stress that survivors experience when being constantly targeted from unknown directions with TECC tactics, research participants also indicate that survivors who disclosed experiencing TECC to their workplaces and civil and criminal legal systems also frequently endured minimization of the abuse. Survivors indicated that supervisors, investigators, commissioners, and other providers seemed to dismiss the seriousness of TECC and its impacts. When this minimization occurred in front of the abuser, for example, during a protection order hearing, survivors indicated feeling further frustration and hopelessness.

Numerous research participants referred to survivors losing faith in the system's ability to help them and that survivors became too fatigued to continue reporting. We expand more on the impacts of the inconsistent and inadequate system's response to TECC in Finding 3.

TECC Contributes to Feelings of Uncertainty

There are many occasions when the accessibility and pervasiveness of technology increases convenience and even safety. However, when abusers use technology to stalk and intimidate, survivors often experience intense disorientation and uncertainty around which tactics the abuser is utilizing. For example, a survivor who participated in this research described numerous instances of her ex-boyfriend showing up uninvited to locations she frequented and she assumed he had accessed one of her accounts. However, she was unsure about the specific point of compromise and whether the abuser has guessed her passwords, used spyware, or pieced together information from social media. This lack of clarity around the breach can create chronic stress for survivors, contributing to the constant state of fear discussed above. Research participants also identified that survivors lacked

“I feel like this is the worst type of terror because you don't know where it's going to come from, you don't know when it's going to happen. You know that it can affect your life long term. Because the thing is, a bruise goes away girl. A bad public image doesn't. So it's worse. I'll take the bruise. I would take the bruise over what I experienced, because it was day in, day out. And just when you think it can't get worse, it gets worse.”

Survivor

reliable resources to consult about their uncertainty and obtain clear information about the point of compromise. Research participants noted that this uncertainty can lead to repetitive checking behavior. For example, one participant described a survivor who was consistently looking through “the most depraved parts of the internet” to make sure her intimate photos had not been posted, while other survivors asked friends to conduct repetitive checks for them.

The lack of clarity around security breaches also makes it difficult for survivors to seek relief from the abuse either through safety planning or formal reporting because of the way experiencing TECC diminishes survivor credibility. For example, if a survivor lacks fluency with understanding how to operate the compromised technology, the survivor may not be able to articulate to providers - such as police, the courts, or advocates - their rationale for believing a breach has occurred. Survivors can find themselves in the position of describing experiences of TECC that sound outlandish and impossible. This can be especially problematic if the provider lacks training in TECC. Research participants repeatedly mentioned instances of providers responding to survivors who described the extent of the abuse as though they were “crazy”.

Research participants also described the way those abusing technology cultivated a perceived expert status. In other words, if the survivor has less knowledge about technology than the abuser, the survivor often automatically confers an expert status to the abuser. Survivors described doubting their own knowledge of their devices and accounts, and experienced intense disorientation about the origins of the abuse. Even if the individual engaging in TECC utilized technologically unsophisticated tactics, research participants indicated that the uncertainty surrounding the point of compromise left survivors conferring a grandiose sense of expertise to the abuser and feeling debilitated by this perceived expertise.

TECC Results in Negative Professional & Economic Impacts

It is increasingly impossible to fulfill job duties without being online as communications, documents, and calendaring are becoming more and more cloud-based. For survivors experiencing TECC, the abuse often spills into the workplace. For example, when an abuser targets a survivor’s work email, ignoring or closing that account is often not an option, thus exposing the survivor to harassing and abusive messages at work. The impact of experiencing TECC at work can also create negative employment consequences, including feeling distracted and having difficulty concentrating on professional tasks. The workplace is often a source of positive reinforcement, social support, and economic independence for survivors. When their job environment becomes compromised, survivors lose another axis of safety.

Research participants described a variety of additional deleterious professional impacts as a result of TECC, such as the stalker leaving false and defamatory reviews about the survivor’s professional performance online and sending real or fabricated intimate images to the workplace. Survivors reported other forms of direct interference with their work, such as their ex posing as potential clients and scheduling dummy appointments with the survivor’s business to clog up her calendar and prevent income generation. Similarly, abusers often access information about survivors through the company’s web presence and professional organizations that the survivor belongs to. Providers who described abusers’ campaigns to discredit the survivor in the workplace noted the ways that domestic violence and stalking has become more “public.”

Interview participants identified ways that abusers rely on technology to perpetuate economic abuse. This may involve identity theft, in which the abuser takes out credit cards and other debts using the survivor’s identifying information. Participants report

that those engaged in stalking would surveil survivors' financial transactions on platforms such as Venmo, which allowed the abuser to monitor financial exchanges, reported activities, and who the survivor spent time with.

The Negative Impacts of TECC are Enduring

When reflecting on the enduring impacts of TECC, research participants described feeling like the abuse never ended. Research participants stated that though the relationship might have ended, along with the physical violence, that survivors experiencing TECC continued to experience consequences and impacts over time. Participants indicated that the threat to distribute intimate images felt particularly unresolved, as survivors reported they had little assurance that the abuser destroyed the images. Survivors also expressed anxiety at the enhanced levels of web searching that employers engage in when hiring a new employee. Survivors who have exited sex trades worried that facial recognition might enable a prospective employer to find ads and intimate images that had been posted or left online without their consent.

Containing information presents an ongoing challenge within the survivor's social networks. Survivors note that even if they implement robust personal privacy settings, they cannot control the stalker's efforts to connect with their friends and family online. Notably, an individual abusing tech can glean a lot from the web presence of the survivor's social circle. Thus, uncertainty for survivors persists over time, as survivors wonder whether the abuser continues to monitor them, resulting in participants repeatedly referring to survivors experiencing chronic stress long after the last contact from the abuser.

“The survivors who I’ve worked with really feel like it’s never going to stop. We’ll be writing up the petition and the person will be texting them while we’re writing it, and they’re like, he probably knows I’m here.”

Advocate

Finding 2: Seattle Lacks a Training & Consultation Structure for Addressing TECC

Research participants indicated a lack of access to training and consultation structures for addressing TECC. Here, we highlight the resulting effects of this gap:

Limitations of Self-Teaching

Research participants identified self-teaching (i.e.: Google) and learning from colleagues as the primary methods by which they gained knowledge about TECC. This inconsistency and lack of formal training proved constant regardless of the provider interviewed or their role (i.e.: advocates, law enforcement, prosecutors). Notably, acquiring knowledge and skill by one's own effort is not itself problematic. For example, K&L Gates founded the Cyber Civil Rights Legal project – which provides pro bono legal services to survivors of nonconsensual pornography – after developing cyber forensic expertise in the realm of corporate law. They realized that their “deep expertise in unmasking people” at the corporate level could fill a gap in legal services available to individuals seeking relief from the unlawful distribution of intimate images.

Rather, the problem with self-teaching as the primary method by which providers currently gain knowledge about TECC is that this endeavor is incumbent upon self-motivated individuals to seek out and acquire skills and knowledge on their own. The limitations of self-teaching are numerous; here we discuss three concerns related to the lack of institutionalized training for TECC as raised by research participants:

Providers Need to be TECC- and Tech-Savvy

Research participants conferred that advocates need ongoing support in learning basic technology safety planning. Some advocates have taken it upon themselves, or received support by agencies, to attend training and obtain TECC-specific knowledge. Other advocates reported discomfort with technology and that they outsourced TECC to

other colleagues. Though it is clear that advocates may, in some cases, need to outsource the intervention around TECC to a more specialized provider, research participants indicated that a baseline ability to assess and safety plan is a fair expectation for all providers responding to coercive control. Within advocacy, research participants highlighted the training that advocates receive around legal systems as an analogous situation; advocates do not provide legal advice or serve in the role of attorney, but they do receive basic training in speaking with someone about legal remedies, such as domestic violence protection orders.

Generational Biases

Related, providers less motivated to seek self-learning opportunities were perceived to hold biases that were influenced by age. Research participants identified judicial officers as exemplar of this particular concern, sharing observations of judges and commissioners requiring in-court instruction from advocates and prosecutors to explain the workings of common social media apps or GPS tracking, and joking that they themselves do not use technology in their personal lives. Judicial officers were not alone in holding generational biases related to TECC-based behavior, particularly in regards to dating apps; research participants noted prosecutor assumptions about dating apps as enabling “hook up culture” played a role in influencing filing decisions, even when (younger) survivors explained their perception of dating apps differently.

Indifference & Minimization

Research participants indicated that the lack of formalized and consistent training among providers reinforces a culture that minimizes the impact of TECC on survivors. The effects of this minimization filter into every interaction that survivors have with

providers; patrol officers who lack training on TECC subsequently fail to identify the pattern of coercively controlling behavior as criminal; prosecutors who lack training on TECC continue to prioritize physical assaults over TECC-based crimes; judges who lack training on TECC continue to identify social media-based harassment as “schoolyard shuffles” and set low bail for TECC-based crimes.

Limitations of Existing TECC-Specific Training Opportunities

Existing opportunities to receive formal training on TECC are inconsistent and often one-off trainings, without follow up to develop expertise. Moreover, as research participants noted, information presented during TECC-specific trainings quickly becomes obsolete. Research participants identified the following as specific detriments to the lack of consistent training opportunities available for TECC:

Training Disparities

Research participants who work within the criminal and civil legal systems indicated that training on TECC (and gender-based violence more broadly) is disproportionately deficient, particularly at the first responder level and when compared to training requirements for other crimes. Research participants regularly referred to the disparity between the training available for TECC and DUI cases, where providers have the opportunity to receive a DUI training certificate to denote specialization in the field and advanced training to analyze and interpret DUI related report data; similar opportunities do not exist for TECC-specific crimes. Research participants identified this disparity in training as contributing to lack of priority that TECC-based crimes receive within the civil and criminal legal systems.

Physical Assaults vs. TECC

Research participants noted that nearly all domestic violence, sexual assault, and stalking cases include some form of TECC. They also noted that without consistent and specialized training for all providers, only a minority of providers develop skill to identify, investigate, and prosecute TECC. Within the

criminal legal system, research participants explain that a resulting consequence of limited training for TECC is that prosecutors move forward with the “easier” physical elements of domestic violence, sexual assault, and stalking cases and the TECC-related behaviors are often not addressed. Research participants acknowledged that investigating and prosecuting TECC-related behaviors is time consuming and resource intensive, yet they also share concern that a lack of training on TECC contributes to the ongoing prioritization of physical abuse over TECC. Additionally, when those who engage in both physical abuse and TECC are only held accountable for physical abuse, research participants expressed concern that abusers learn that the criminal and civil legal systems excuse TECC, thus signaling to abusers that this behavior is defensible.

Training & Workplace Culture

Troubling for many research participants concerned the recognition that TECC-specific training would require a significant time commitment over an indefinite period of time; research participants recognized that because TECC constantly evolves, a formal training curriculum would require follow up trainings and regular updates to materials and practices. Research participants expressed apprehension about attending trainings because of high caseloads and the stress of falling behind, even to attend one, day-long training. Although nearly all providers expressed this sentiment, advocates – particularly systems-based advocates – expressed concern about burnout, the challenges to continue professional growth, and to develop advanced knowledge in the field when prioritizing the day to day workload. Research participants also identified the inflexibility of the court calendar as another barrier to taking advantage of training opportunities.

Training on Helpful Technology

Research participants also cited positive uses of technology, especially in the context of enhancing a survivor’s safety plan or as investigative tools, yet advocates and other providers noted they lacked a structure for learning and sharing knowledge about

these helpful forms of technology. Participants reported survivors using a variety of tech-based strategies to increase their safety and access to resources, including using home security systems for video surveillance, smartphones to record respondents violating protection orders, and Google Translate to increase language access. Research participants also explained that in some cases, law enforcement agencies limited the number of counter-surveillance accounts within a unit (i.e.: Facebook and other social media platforms) and this especially impacted new hires. Other participants noted infrequent training opportunities for other helpful forms of technology, such as Law Enforcement Information Exchange (LINX) access for patrol officers. Without an opportunity to complete this training, patrol officers are unable to utilize the LINX program, which allows officers to access and view reports filed in other jurisdictions. In the context of TECC as a pattern-based crime, research participants identified this as a particularly critical training gap.

Institutional Knowledge & Provider Turnover

Self-motivated, curious, compassionate, and empathetic providers have developed a wealth of individual expertise in the area of TECC. However, without consistent unit-wide training or comprehensive onboarding when new providers join units, as individuals with expertise transition to new positions and different units, their expertise leaves with them. Regular provider turnover creates a multi-fold problem, exemplified across units. Here we highlight the way turnover impacts the Seattle City Attorney's Office:

Participants described that SCAO prosecutors serve short (approx. two year) rotations within the DV Unit. They arrive not as a cohort, but individually at various points throughout the year, making a unit-wide onboarding training structure challenging. Without a cohesive onboarding structure for new prosecutors, research participants noted that it is difficult to establish the unit's values and approach to prosecuting misdemeanor domestic violence crimes, in addition to developing expertise in the

area of TECC. While prosecutors serve short rotations, the SCAO advocates remain in their roles over time, thus accumulating and retaining the institutional knowledge of the unit. While appreciated and highly proficient, advocates end up serving as unrecognized and uncompensated de facto trainers for the prosecutors, adding an extra layer of work to the advocate's already high case load.

Lack of Consultation Structure for TECC

Across scale - from individual unit, to the city of Seattle, to King County and beyond – informal, ad hoc information sharing is the current consultation structure for TECC. This informal sharing often relies on interpersonal relationships established over time or across units proximal to one another; for example, a prosecutor will call a former colleague with expertise in TECC who transitioned to another unit, or an SPD detective in the DV Unit will take the elevator to the Cybercrimes Unit to ask for assistance in deciphering a cell tower report. While providers calling colleagues or professional acquaintances to obtain immediate information is often effective, this is also an inefficient way to share and obtain information – particularly materials that all providers might benefit from having access to, like TECC-specific safety plans and templates for warrants. This informal information sharing structure also has potential to place an added burden on colleagues who are responsible for other work. The region also lacks a staffing structure for TECC-specific cases, presenting a gap in opportunity for providers to learn from one another, report back on how cases resolve, share lessons learned, and collaborate on cases that cross jurisdiction.

In addition to the lack of internal consultation structures between community and system professionals, the current absence of direct consultation relationships with technology companies creates barriers to effectively respond to TECC and survivor needs. Research participants noted the inability to consult directly with tech companies as a specific challenge. For example, tech companies and platforms do not typically provide contact information to community and

and system professionals, thus leaving providers with no direct means to ask questions specific to the platform, understand a company's standard for taking action in response to harassment and abuse, or request the take down of material on behalf of a survivor. Though many companies may have designated law enforcement compliance contacts, these contacts do not necessarily assist a community-based advocate in answering questions, nor someone seeking civil relief, such as a protection order. Research participants also described an inefficient trial and error process to determine who to ask for information within a company and often file numerous warrants with minor changes until landing on the specific language to access evidence-related data that a tech company requires. Research participants also identified inexcusably long wait times to receive data requested through warrants. One prosecutor reported resorting to using LinkedIn to identify the CEO of a tech company, and then guessing an email address formula for the company combined with the executive's name (I.e. John.Doe@techcompany.com) in order to get a response to inquiry.

“When I came in, I still used a typewriter.”

Detective

Finding 3: Seattle’s Response to Address TECC is Inconsistent & Inadequate

Interviews with research participants revealed a need for more robust solutions to TECC. Fundamentally, survivors want the abusive behavior to stop and lack access to effective mechanisms to achieve this goal.

The Survivor Experience

To begin, survivors of TECC are not commonly mired in the criminal legal system due to an unwanted mandatory arrest. Instead, these survivors are actively seeking relief from the legal systems and often fully engaged as participants in the reporting and investigative process.

Research participants raised concerns that the civil and criminal legal systems response is inconsistent when survivors attempt to report TECC concerns. For example, survivors often report single incidents of TECC as they occur. Survivors indicated that the responding patrol officer might take a report to document the incident, but not do additional follow up or investigation afterward to link the incidents. Survivors conveyed that they wished they could communicate directly to a detective to explain the totality of the circumstances. Jurisdictional issues also compounded the stress of survivors seeking support from the criminal legal system, due to a lack of cross-jurisdictional information-sharing. One survivor reported that she had made six incident reports in three different jurisdictions in King County, and none of the agencies linked the incidents or recognized the pattern and scope of behavior. The survivor’s own efforts at trying to explain the totality of behavior gained no traction. For survivors with experience reporting incidents in different jurisdictions and engaging with different agencies, they identified that their concerns were prioritized differently depending on the jurisdiction, noting that in some jurisdictions, patrol officers appeared busy prioritizing imminent physical violence and less busy jurisdictions seemed to have more time to devote to investigating cyberstalking.

Survivors who participated in this project reported

exhaustion, disillusionment, and frustration with institutional responses to TECC. The documentation of stalking is labor intensive. Survivors spend significant time screen capturing numerous contacts, creating logs, searching for their intimate images on “revenge porn” websites, and researching different phone anonymizing apps to try to ascertain which one the abuser is using. Numerous advocates cited survivor attrition. Survivors feel the system is unresponsive or minimizes their complaints regarding TECC, even in cases where there is a protection order or no contact order in place and a history of violence. When the individual engaging in TECC resides out of state, advocates reported survivors feel especially powerless. Some survivors stop reporting altogether, whereas research participants explained that others leave the city rather than rely on the local systems for help. Importantly, when systems did hold those abusing technology accountable, participants reported survivors felt a “huge sense of relief.”

Investigative Challenges

Providers spoke to the overall challenges to investigating TECC cases. Here, we focus on the specific challenges in supporting the successful investigation and prosecution of misdemeanor TECC cases. These challenges center on a multi-tier problem: TECC cases often require significant investigative resources, yet misdemeanor level cases rarely receive advanced investigative support, and the level of investigation that TECC cases require often exceeds the resources, training, or skill level of patrol officers. For example, if someone abusing technology takes even basic steps to disguise their identity - such as blocking numbers or creating dummy accounts - the investigator must obtain warrants to different platforms in order to

establish and authenticate identity. Providers indicated that this is a time consuming and resource draining process, which often requires submitting additional warrants and months of waiting before receiving data from the tech company. The lack of investigative support is of particular consequence regarding the disclosure of intimate images cases, as this a misdemeanor for the first offense in Washington. If the individual distributing the images has disguised their identity, it can be almost impossible to unmask the abuser at the patrol level. At the time of this research, the Seattle Police Department assigned one misdemeanor detective to the Domestic Violence Unit. In 2018 the Seattle City Attorney's Office received 3,600 referrals and filed 2,000 cases; it is self-evident that one detective cannot shoulder this volume of work.

Consequently, many reports of TECC end up nowhere—they are documented by patrol, lack sufficient investigation to build a case, and are deemed too insubstantial to file charges. The abuser often has no interaction with an officer, while the survivor expends time and energy seeking relief that rarely arrives. This is also troubling because survivors indicate that they continue to experience TECC for months and even years, and providers indicate that those engaging in TECC are often repeat offenders with prior victims. The inconsistent and inadequate response to TECC results in missed opportunities for early intervention, before the behavior escalates to a felony or the abuser moves on to a new target.

Notably, systems-based advocates - advocates located in police departments, prosecutors offices, and the courts - play a critical role in supporting misdemeanor level TECC cases. They often provide context to the prosecutor about the survivor's experience and serve as the keepers of "institutional memory" in the City Attorney's Office. For example, an experienced advocate might recall investigative strategies from a prior successful case that could advance a current case, whereas a newer prosecutor may be unfamiliar with such strategies. However, providers also indicated that systems-based advocates and prosecutors sometimes fill investigative roles in their own cases and that this role confusion contributes to the inconsistent and inadequate system response to TECC. While systems-based advocates and prosecutors both acknowledged that they should not be conducting investigations and interpreting digital data, they were without additional investigative support to build a comprehensive case against TECC offenders. Additionally, providers also mentioned cobbling together different charges to elevate the case to a felony in order to get sufficient support. This practice presents concerns as often a misdemeanor level response would suffice, and inflating the charges may lead to a gratuitous level of systems involvement. Overall, both practices speak to the challenges providers face when trying to support survivors in misdemeanor level cases.

“When I think back now, there were probably a lot of cases that could have been solved on patrol instantaneously, had there been more, more access to these systems.”

Law Enforcement on LInX

Evidentiary Standards for TECC

Research participants indicated confusion about the necessary level of evidence to move TECC cases forward into the system. This confusion creates a chasm between accessible, low-threshold ways for abusers to engage in TECC and what research participants perceive as an impossibly high threshold to hold those doing harm accountable. Providers raised concern that the perceived challenges to authenticating identity and locating the source of abuse overshadowed other creative ways to build a case. Participants mentioned feeling that prosecutors disregarded the patterns of TECC within a case and disproportionately emphasized proving one small component of abuse. For example, an advocate cited a case that involved an abuser sending unwanted messages to the survivor from his Facebook account. Rather than building a case around the broader pattern of stalking and common verbiage that the abuser used in all of his harassing communication with the survivor, the case became about proving that it was the abuser sitting at a particular device, sending a particular message, from a particular account, in a particular moment. In other words, the case became about proving a single incident versus looking at the totality of the pattern of harassing communication. Further, providers indicated that the primacy placed on the authentication process meant that prosecutors rarely moved forward in cases when the person doing harm used a spoofing application.

Additionally, providers found it troubling when prosecutors framed decisions to decline filing in TECC cases because of “resources” as opposed to victim impact. Providers indicated it a dangerous precedent to establish TECC cases as too time intensive and not worth the drain on resources when the damage and impact of TECC has been so clearly established. Finally, providers reported that it felt dispiriting to receive notice that the prosecutor’s office declined to file on a TECC case shortly after the officer filed the report and knowing that no additional investigation had taken place. Providers

identified this as reinforcing confusion over filing standards and practices, and the overall perception that the system minimizes TECC.

The Protection Order Experience

The inadequacy of the current protection order process as it relates to TECC is distressing. At the time of this research, no accessible system exists to enter digital evidence into the court record and petitioners continue to file by paper.

The inefficiency of the current system is a problem not only for survivors of TECC, but for every King County stakeholder involved in this issue. Research participants provided an overwhelming number of examples to support this finding. Providers noted that judicial officers spend significant amounts of time deciphering petitioner handwriting when kiosks might be made available to help with crafting typed petitions electronically. Providers also indicated that the ability to craft orders electronically would improve the ability for parties and law enforcement to read findings in the orders. Providers noted the discrepancy that E-Orders are available in some proceedings in the same court building, but not in civil protection order proceedings.

Research participants raised concerns about the way the paper-based filing structure of the civil protection order process fails as a platform for tech abuse and the preservation of digital evidence. Providers described instances of survivors transcribing audio files containing abusive messages because there is no current system to consistently upload digital evidence into the record. The current system also requires survivors to screen capture text messages or use paid software to download text messages in their chronological order. Survivors then must print the messages (upwards of hundreds or thousands of messages), only to file the petition with court administrators who must re-digitize and scan the evidence back into the court record. This can present a troubling equity issue. Survivors who have access to office supplies and who are comfortable organizing such materials might be more successful in the protection order

process compared to those who lack such access and experience, regardless of the abuse they are enduring.

Research participants indicated that video evidence is largely unconsidered by the court, despite its evidentiary value. In one case an attorney created a password protected YouTube channel for the commissioner and parties to view the video that contained evidence of abuse, and the commissioner declined to view it. When electronic evidence was presented to the court on a flash drive, numerous providers stated that judicial officers would not consider this evidence. Providers cited concerns about viruses on flash drives and a lack of clarity around how to incorporate this evidence into the official court record.

Another provider recalled a case in which the respondent in a Domestic Violence Protection Order filed intimate images of the survivor into the court record and the commissioner did not grant the petitioner's request to seal the record. In this instance, the intimate images became public record and the court became a forum to perpetuate abuse and illegal behavior. Providers also identified a lack of consistent and clear language in protection orders around prohibiting the distribution of intimate images. Research participants also referred to significant barriers in the service of orders; personal service can be inefficient, especially when a respondent is evading service. Survivors reported missing work related to continuances associated with service challenges. The inability to serve by text or email is especially grating to survivors experiencing TECC, as they know the respondent is regularly on their device and using it to cause harm. Overall, these inefficiencies can exacerbate trauma.

“If you go back in the story, you'll see it was a 911 report, and nothing happened. And that's really unfortunate because it just sends a variety of bad messages to the victim, you know, to the community, to law enforcement.”

Prosecutor

Finding 4: Seattle Lacks Sufficient TECC-Specific Prevention Education and Community-Based Resources

Research participants concurred that Seattle currently lacks sufficient TECC-specific awareness raising and education programs and that this absence is rooted within the way the community discusses personal safety and security. For example, a technologist noted that children often learn about “stranger danger” from a young age and that adults (especially women) are inured to implement personal physical safety plans when traveling or walking in public space. Yet, neither children nor adults receive regular education on how to implement or increase personal security in cyberspace, even as our professional, personal, and financial lives increasingly rely on digital technology for everyday communication and activity. This lack of TECC-specific prevention education has led to a gap in basic understanding of the technology that we use, and it is often not until we experience an unanticipated security breach that we appreciate the gravity of our narrow conceptions of personal safety.

The Repercussions of Late-Start Youth Prevention Efforts

Research participants indicated that current TECC-specific prevention efforts begin too late and that children and young adults are already using technology before receiving education on how to protect their digital information and what constitutes online harassment and abuse. In other words, youth have already been exposed to risky online practices and a culture of online harassment before receiving TECC prevention education. Additionally, research participants identified a lack of resources and tools to assist parents in engaging their children in discussion about online safety. Advocates also acknowledged the difficulty in engaging children of survivors in discussion about tech safety planning, particularly when the survivor’s safety plan is affected by the child’s online behavior.

The Invisibility of Private Sector Technology Companies

In discussing the lack of sufficient TECC-specific prevention education available within the community, research participants raised concern about the perceived indifference among technology companies and their role in educating the public on the ways their products and applications could be misused. More explicitly, research participants indicated that private sector technology companies have a responsibility to engage in broad-based awareness raising campaigns to educate the public about tech safety and that their current lack of engagement in prevention education reinforces their role in facilitating TECC. Beyond the role of technology companies, providers also identified a gap in participation among private sector tech employees, particularly those who could serve as expert

witnesses in civil and criminal court proceedings, thereby contributing to enhancing the public's understanding of TECC.

Insufficiency of Community-Based Resources for Survivors of TECC (Material)

As community-based agencies continue to respond to survivor's physical, financial, and emotional safety needs, research participants noted a gap in resources pertinent to survivors experiencing TECC, namely the ability to replace or repair compromised technology. Safe and secure smartphone access represents a lifeline for many survivors, particularly survivors who rely on smartphones for not only their daily personal and professional communication needs, but who run their independent businesses through their smartphones and who do not otherwise have regular computer and internet access. While community-based agencies continue to distribute Hopeline phones donated by Verizon and this program provides a critical resource in time of crisis, these phones are traditionally "flip phones" or "burner phones" without internet network access. In addition to smartphones, research participants noted a need for more legal services and attorneys that specialize in TECC. While the Cyber Civil Rights Legal Project provides pro bono, specialized legal assistance to survivors who have experienced nonconsensual pornography and the distribution of intimate images, research participants also identified the need for attorneys with specialized TECC knowledge to represent survivors in civil cases, including protection order hearings and family court proceedings.

Insufficiency of Community-Based Resources for Survivors of TECC (Consultative)

Research participants identified gaps in consultation services to support survivors of TECC, namely a lack of trained specialists with knowledge of power-based relationship dynamics to provide technical assistance to survivors whose phones, tablets,

computers, and accounts had been compromised by their abuser. More specifically, research participants identified a need for one-on-one consultation services to assist survivors in identifying points of compromise on devices, to conduct spyware scans, and to develop safety and mitigation plans in response. While tech support services exist (i.e.: Best Buy's "Geek Squad" or Apple's "Genius Bar"), research participants noted barriers for survivors in accessing these services, including fear of not being believed and dismissed as "crazy". Advocates also identified a gap in direct consultation opportunities with tech companies - specifically a lack of direct customer support for social media platforms and websites that enable the distribution of intimate images. While we note the lack of consultation with tech companies in Finding 3, we highlight this issue again here, as advocates described how the inability to consult directly with tech companies contributes to ongoing personal and professional impact for survivors attempting to initiate take down requests to remove intimate photos or regain access to accounts.

Insufficiency of Community-Based Resources for Survivors of Acquaintance or Stranger TECC

While Seattle lacks sufficient community-based resources for survivors of TECC in general, the inadequacy of resources compounds for survivors of TECC who are targeted by someone other than an intimate partner. Providers cited instances of survivors being targeted by acquaintances or strangers via technology. While domestic violence specific providers indicated they would provide support, safety planning, and resources for survivors of acquaintance or stranger TECC, they also noted the lack of relationship status may prevent these survivors from knowing these resources were

³We conducted the majority of interviews for this project (summer 2018) before the TECC Clinic – a free clinic developed in collaboration with members of the TECC Working Group and hosted by New Beginnings – had launched; most research participants were unaware of plans to develop this community-based initiative to support survivors of TECC.

available. For example, first responders often struggle to identify TECC within intimate relationships and providers suspected that first responders would be less likely to refer a stranger cyberstalking case to a community-based domestic violence agency. Similarly, providers noted that acquaintance and stranger TECC cases reported to law enforcement do not always receive an assigned systems-based advocate. Similarly, survivors of acquaintance or stranger TECC may not be aware of community and systems-based domestic violence advocacy services. Given the Protection Order Advocacy Program is designed to provide support for petitioners seeking Domestic Violence Protection Orders, there is not the same level of support for those petitioning for Anti-Harassment or Stalking Protection Orders. Thus, a survivor will not necessarily know that an Anti-Harassment Order does not carry the same protections as a Stalking Protection Order. One survivor interviewed reported making over 30 reports of violations of her Anti-Harassment Protection Order before eventually learning she could petition for a more robust order.

“This is something that I sort of knew distantly about, but definitely became more familiar with just volunteering, is the degree to which survivors are doubted or disbelieved and I feel like that would be a really important thing just to start from a place of okay, we don’t know how this is happening, but I’m listening to you...You are not making this up.”

TECC Clinic Volunteer Technologist

Recommendations

In this section we cohere the recommendations provided by research participants for improving Seattle’s response to TECC within five interdependent and overlapping themes. A key element of each recommendation concerns the integration and centering of TECC into all aspects of Seattle’s response to domestic violence, sexual assault, and stalking. The interdependence of TECC and other forms of abuse must be recognized in order to effectively respond to the needs of survivors.



Recommendation 1: Improve Regional Partnerships and Collaboration

Providers identified a desire for increased communication and exchange within and across units noting such partnerships would help clarify expectations and procedures among the different providers who respond to and support survivors. For example, law enforcement identified interest in increased communication with prosecutors to clarify evidentiary standards for filing; prosecutors identified interest in providing warrant templates for law enforcement; advocates identified interest in increased communication with the Department of Corrections to clarify offender supervision plans. Advocates also identified interest in increased communication with law enforcement to clarify investigative expectations and with judicial officers to clarify expectations around evidence and authentication standards for protection orders.

To establish increased communication and collaboration across units, we recommend the following:

Designate a Centralized TECC Consultation & Technical Hub

We recommend establishing a robust and institutionalized consultation and resource sharing structure for all entities involved in the response to TECC. To standardize communication and collaboration across units, providers proposed establishing a centralized unit responsible for housing and maintaining shared resources related to TECC. We recommend drawing on already existing expertise in this area and expanding the Special Operations Unit to serve as the centralized and designated technical and consultation resource within King County for TECC-related issues. This centralized TECC hub could maintain resources, templates, and materials that would be stored and made available on a shared resource drive to relevant providers and develop, maintain, and staff listservs where providers, including advocates, can pose questions and the entire listserv community benefits from the responses.

Institutionalize a Regional TECC Multi-Disciplinary Task Force

We recommend the Centralized TECC Consultation and Technical Hub implement a Regional TECC Task Force to support the investigation of TECC-related crimes throughout King County. This Task Force would pool expertise across jurisdictions to develop a highly trained group of law enforcement officers and prosecutors to assist in cross-jurisdiction investigations or provide additional support with specialized TECC prosecutions. As a means of supporting agencies with fewer resources across the region, we recommend this advisory group adopt a SWAT or narcotics team approach that recruits one person from smaller agencies who serves as the designated representative to the task force. We also recommend exploring how existing units might be better utilized to support this task force, including the Seattle Police Department's Intel and Cybercrimes Units. We envision that these specialized TECC investigators and prosecutors would support each

other's work, develop best practices for investigating and prosecuting TECC crimes, and also serve as a resource to the broader community. We recommend that the Task Force include advocates and civil attorneys who represent survivors' interests. The Task Force will respect the confidentiality of different disciplines, and all members of the Task Force should be able to set agenda items for discussion.

Institutionalize Collaboration Between Public & Private Sectors

We recommend institutionalizing partnerships between the public and private sectors, including establishing direct communication channels between providers and tech companies. Direct communication will buttress the efficiency and effectiveness of those working to support survivors within both advocacy and investigations. Institutionalizing a collaborative consultation and communication structure will also provide opportunity for potential information sharing when the individual abusing technology is an employee of a tech company. Providers also identified interest in more robust communication and information sharing with tech companies to communicate concerning trends regarding how the company's platform is being abused, or to glean insight from tech companies regarding processes for the take-down of intimate images or removal of harassing content. We also recommend increased direct communication between the public and private sectors to recruit and train a potential pool of expert witnesses for civil and criminal proceedings.

“...if we prioritized things differently, you know, giving a little more priority to these cases as opposed to bike theft cases. I mean, I understand that's an issue too, but so far, in my 18 years in law enforcement, nobody has died as a result of a bike theft.”

Detective

Recommendation 2: Increase Consistency of the System Response to TECC

To establish a more consistent and effective response to TECC, we recommend the following:

Implement TECC-Responsive Protocols & Assessment Tools

First, we recommend that providers consider and assess survivor impact at every interaction they have with survivors. Fear and emotional impact are elements of (cyber)stalking and should be consistently considered by those in investigative roles. In other words, prosecutors, judicial officers, and other decision-makers and fact finders must consider survivor impact - as opposed to only lethality - when determining whether to file charges, allocate resources, or issue a protection order. Experiencing TECC has resulted in survivors losing their jobs, a sense of safety, and their public reputations and we must frame the system response beyond physical violence to capture the totality of abuse that survivors experience.

Second, we recommend agencies and units integrate TECC into all existing assessment strategies and protocols. Thus, rather than distinguishing between "cyberstalking" and "stalking", these behaviors would be seen as

equivalent and inextricable from one another. For example, if an advocate is developing a safety plan with a survivor, TECC should be continually assessed for and addressed in the safety plan. Similarly, if an officer responds to a complaint involving technology, the officer should consult TECC-responsive protocols and assessment tools to encourage appropriate digital evidence collection and preservation. More specifically, in regards to the patrol response to TECC, providers referenced the DUI protocol as a model for developing a TECC-responsive patrol protocol. Providers repeatedly referred to the benefits of the DUI protocol in increasing the consistency of patrol responses to DUIs and believed a similar protocol would create a more consistent and effective patrol response to TECC.

As part of a TECC-responsive patrol protocol, providers recommended that patrol officers initiate a conversation with survivors about whether or not they want the suspect contacted and told to "knock it off". Providers indicated that "knock it off" conversations serve multiple purposes, first placing

"How do we figure out a way that our system can respond appropriately so that it's not an intern having to take all these extra steps, but that there's, there's a clear protocol? Like oh! This is what we do when we hear this. These are the steps, and this is how we triage...so it's not based on just the, whoever's lap it falls into and their own discretion."

Advocate

the individual abusing technology “on notice” that their behavior is unacceptable and causing the survivor distress. Second, by documenting these conversations, they assist in establishing a pattern of stalking behavior (and its emotional impact) should the person abusing technology continue with the unwanted contact. Providers acknowledged that too often the burden falls on the shoulders of survivors to continue reporting and that patrol officers rarely obtain statements from those abusing technology. Notably, providers indicated that the particular circumstances of the situation and a survivor’s safety plan should be taken into consideration, and that “knock it off” conversations might not be appropriate in all cases, and should not replace a thorough suspect interview if a survivor wants a case to move forward.

Third, we recommend developing a triage system to determine case prioritization. We suggest drawing on the knowledge of providers with training in threat assessment to assist in developing a triage system that is attentive to abuser typology. Providers identified interest in deprioritizing low level, low risk cases, particularly those where survivors do not want systems intervention. Consequently, we recommend a triage system that prioritizes pursuing cases with active survivor participation and cases involving offenders with a history of multiple victims.

Taken together, the implementation of TECC-responsive protocols and assessment tools will provide opportunity for earlier intervention and a triage system that prioritizes cases based on lethality and survivor impact.

Role-Specific Recommendations

In addition to implementing TECC-responsive protocols and assessment tools into the current response to TECC, providers also identified recommendations specific to individual agencies and units:

Increased (Misdemeanor) Investigative Support

Providers identified a need for increased investigative support in TECC cases, particularly

misdemeanor-level TECC cases. Providers specifically noted the need for increasing investigative support within the Seattle City Attorney’s Office (SCAO). Providers also identified a need for additional resources to support TECC investigations, specifically recommending the expansion of department issued smartphones for documenting and uploading evidence, offering additional Law Enforcement Information Exchange (LInX) trainings to allow more patrol officers access to LInX to assist with misdemeanor-level investigations, and approving additional detectives for department authorized Facebook and other social media accounts for counter-surveillance purposes. Providers also recommended developing best practice investigation and prosecution strategies to address authentication of identity challenges and to develop more offender-focused investigative strategies to reduce the burden on survivors in TECC investigations.

Prosecutor Practices

In response to providers who identified confusion around inconsistent filing standards for TECC cases, we recommend prosecutors develop and distribute filing standards to appropriate stakeholders. Providers located in law enforcement recalled that while on patrol, they would typically only receive decline letters from SCAO, which often felt dispiriting. Receiving information about successful cases would provide patrol officers with a more complete perspective on evidentiary standards for filing. While we recognize that high workloads prevent the prosecutor’s office from currently crafting more detailed communications, we do recommend the prosecutor’s office consider alternative formats for conveying the status of a case. Providers recommended that domestic violence prosecutors make filing decisions in domestic violence cases. Particularly with TECC cases that involve a pattern of behavior that often persists over time, providers indicated that the consistency of one prosecutor following a case from filing to trial proves valuable.

TECC-Specific Offender Supervision

Providers recommended reevaluating supervision plans for offenders in ways that centered the restriction of offender's permitted online use. We recommend borrowing from the current strategies to supervise offenders of online child pornography. While we recognize that offenders of TECC may require internet access to conduct job searches, providers also indicated that the most effective punishment for those who abuse technology is to limit their access to technology; providers referred to this prohibition as "internet jail". We also recommend implementing a case management approach for TECC cases to determine when continued supervision might be desired and that survivor impact – not only lethality - should be a consideration in ongoing supervision. Finally, as noted at the time of this research, the jail lacked a protocol for video calls; we recommend closing this gap and implementing a protocol that addresses this new technology.

Long-Term Legislative Change

Providers also acknowledged gaps in the current Cyber Crimes Act that require attention. While we realize legislative change occurs over time and entails compromise, we recommend stakeholders consider the efficacy of addressing cyber-related crimes within the broader pattern of coercive control that does not entail technology; in other words, we encourage stakeholders to consider the unintended consequences of distinguishing cyber-related crimes as distinct from a broader pattern of "traditional" stalking and harassment. We also recommend stakeholders consider establishing the distribution of intimate images as a felony; research indicates that harsh criminal penalty serves as the most effective deterrent to this particular crime (Eaton et al 2017). Finally, we recommend consulting with tech companies and tech experts to anticipate emerging forms of technology to allow for new TECC-inclusive laws to be as responsive as possible to the evolving tactics of those who abuse technology and the experiences of survivors.

"[Phone-based harassment] is the most common, but it's also really difficult to prove, because you need additional follow up to prove, did this person actually send the communication? And so those are, even though they're the most common cases, they are also cases that are least likely to be filed."

Advocate

Recommendation 3: Implement Standardized & Consistent Training Structures

We recommend the implementation of standardized and consistent training for all providers involved in the response to TECC that accommodates the varying sizes, schedules, and cultures of these entities and agencies. In other words, we do not recommend a one-size-fits-all approach to training on TECC, but rather diverse training platforms and models best suited to providing units with regular and up to date information.

Regular Training for Providers Responding to TECC

Providers recommended a range of ideas to fulfill this individualized training structure and emphasized that all training plans should include regular updates and boosters as technology is ever-evolving. Advocates should have access to training focused on TECC-specific safety planning strategies and standing opportunities to attend professional conferences and/or webinar series that advocates could engage with at their convenience. For all systems professionals, we recommend that training emphasize survivor impact. Lethality should not be the only factor that investigators, prosecutors, and commissioners consider in system intervention efforts, especially when survivors make multiple reports and experience a drastically decreased quality of life, all while those doing harm become more sophisticated and entrenched in their tactics.

Providers consistently reported that in-person training can be a challenge for patrol schedules. As an alternative, provider recommended utilizing existing briefing times for trainings, including developing a video roll call training for patrol officers that would cover evidence preservation and investigative strategies for TECC-involved cases. For new officers, we support the recent efforts of the Seattle Police Department to incorporate Cyberstalking content into Post-Basic Law Enforcement Academy.

Prosecutors and detectives responding to TECC may need protected time to ensure opportunities to receive training, align strategies, and develop a designated repository for templates and tools, such as a SharePoint. Developing open source investigative techniques, fostering ways to communicate with tech platforms, and establishing best practices to investigate and prosecute TECC cases also serve as self-teaching opportunities that will continue to expand prosecutor and detective expertise in the area of TECC. We recommend updating resources for judicial officers, including the Domestic Violence Manual, to include explanatory content about different platforms and social media. Tech savvy attorneys or tech companies could assist in drafting these resources. Research participants also suggested developing new TECC-specific “pocket briefs” that could be filed with a case, if needed. Whenever practical, in-person trainings should be filmed and archived so that allied professionals can access them at a later date.

When determining content for trainings, organizers should look to both local experts and the national landscape. Other regions may be approaching these same issues from a different perspective and have wisdom to share. Advocates might consider attending the National Network to End Domestic Violence Annual Tech Summit Conference, which focuses specifically on these issues.

Training on Helpful Technology

As noted, providers rely on a variety of helpful technologies to support survivors. We recommend that providers receive regular training on responding to TECC, including forms of technology that might assist them in better supporting survivors and/or holding those who abuse technology accountable. For advocate training, we recommend incorporating the use of helpful technology that might better support developing survivor safety plans. Consistent training opportunities could help advocates incorporate new tools and resources, such as security systems and safety apps, into their safety planning practices, while balancing conversations around any unintended consequences of the technology. We also recommend increased use of resources such as the Law Enforcement Information Exchange (LEIX) that would better help officers connect single incidents of TECC with the broader context of coercive control. Given that many survivors live, work, and play in different jurisdictions across King County, it's critical that officers have the ability to view other reports the survivor has made about the same behavior.

Recommendation 4: Enhance TECC-Specific Prevention Education and Community-Based Resources

To increase community awareness of TECC, and to prevent individuals from experiencing and engaging in TECC, we recommend:

Expand TECC Responsive Primary Prevention Training

Research participants mentioned wishing there were more preventative resources around tech safety for the community. Specifically, numerous providers described working with survivors who wished that they had knowledge of tech safety precautions, such as robust password management systems, to prevent account compromise. To that end, we recommend that TECC-specific education and bystander intervention training be incorporated into current primary prevention programming, curricula, and campaigns.

We recommend that standing best practices in primary prevention, such as the socio-ecological approach, address this concern at individual, interpersonal, community, and societal levels. For youth-focused programming, we propose models that discuss digital consent⁵ in relationships. This is a mechanism to proactively address norms around frequency of online communications, picture sharing, and other behaviors that can become coercive. We propose that bystander intervention focus on prosocial norming. For example, if someone's intimate images are distributed without their consent, TECC-inclusive bystander intervention and prosocial norming would condemn the boundary violation, support the survivor, and discourage further distribution. We recommend the integration of technology safety trainings into other prevention content and materials as a reflection of how youth communicate. We propose the expansion of any existing prevention efforts in the community that already address these concerns. In addition to youth-focused training, training should be made available to survivors currently receiving or

seeking services related to intimate partner violence, sexual assault or stalking. This training could promote awareness of digital privacy, as well as ways that technology might support a survivor's safety plan.

Awareness Campaigns with Tech Company Partners

We support and recommend developing outreach campaigns in collaboration with tech companies that promote awareness about privacy features and include efforts to better help parents understand the technology that their children are using. There can be a chasm between a parent's comfort level with technology, and that of their child. This chasm can intensify if a parent is seeking safety and has concerns about being stalked via technology; it's critical that survivors know how to have safety and privacy conversations with their child. Participants identified that tech companies play a crucial role in such outreach campaigns. They have a responsibility to their consumers to help ensure a safe user experience. It is critical to consider cultural competence and language access in the development of any of the aforementioned training and outreach efforts.

Supporting Community-Based Agencies to Integrate TECC Responsive Programming

Participants identified the need to build capacity amongst community-based agencies to respond to TECC. This involves incorporating TECC responsive safety planning strategies into advocacy. Professional development training must also be

⁵See for example the National Sexual Violence Resource Center's digital consent resources: <https://www.nsvrc.org/i-ask-digital-consent>

made available to advocates on a regular basis. Given the way that technology and its ability to abuse constantly adapts and evolves, training must be ongoing and updated.

Supporting and expanding TECC Volunteer Clinic Programs across the region, such as the clinic currently offered by New Beginnings, represents one community capacity building strategy. The TECC Volunteer Clinic began in October 2018 and completed a successful six-month pilot. This clinic pairs a volunteer technologist, trained in the dynamics of coercive control, with a survivor seeking assistance around their technology. The volunteer helps the survivor identify the point of compromise on their device(s) and works with them to develop a mitigation plan. At the time of this writing, 34 survivors received specialized tech safety support and they report positive experiences following their clinic session. For example, 92% of survivors who completed the post-clinic survey reported that they “agree” or “strongly agree” that they knew more strategies for protecting their privacy and information after meeting with the technologist, and 100% of survivors indicated that they “agree” or “strongly agree” that the technologist who they worked with listened to their concerns, was patient and helpful, explained things in a way that they could understand, and had lots of ideas and suggestions. Survivors have complex needs around technology and working with a trauma-informed specialist, in an appointment dedicated to those questions, represents a critical component of their safety plan.

We also recommend the promotion of creative uses of flexible financial assistance as another strategy to address survivor resource needs. Many local programs have funding for mobile flexible advocacy, and we support the expanded use of such funds to provide material support to survivors, including help purchasing a new smartphone, computer repair, hard drives to backup evidence, and in-home security systems.

“It's really important to empower survivors on how to use technology to gain more control of their lives. That as we continue this journey, we're not vilifying the tech.”

Advocate

Recommendation 5: Implement Protection Order Modernization Project

The insufficiency of King County's Protection Order process - as it relates to TECC - requires its own focus and action. At the time of this research, no accessible system exists to enter digital evidence into the court record and petitioners continue to file by paper. Research participants repeatedly referred to the paper-based nature of the current, civil protection order process as problematic given the modern age of tech-based communications. Research participants also raised concern about the potential for liability as the current system's inability to receive digital evidence represents an equity issue for petitioners, particularly for those whose only evidence is digital. The inefficiency of the current system is a problem not only for survivors of TECC, but for every King County stakeholder involved in this issue.

We recognize modernizing the current protection order process will require a broad coalition of stakeholders and potentially legislative fixes, and that the scope and magnitude of this work will take time to implement. We believe the long-term benefits of modernizing the protection order process are worth these efforts. Thus, we provide long-term recommendations for modernizing the protection order process, as well as short-term interim suggestions to improve the current protection order process. We also recommend commissioners and judges develop a standardized best practice for limiting the inclusion of intimate images in the public record; when the court permits intimate images into the record without putting protections in place, the court is perpetuating abuse by enabling the distribution of intimate images.

“I've had more than a handful of victims who have just moved. They'll change their number. They'll leave the city, they'll -- some of them have left the state, just because it's easier to start over than it is to rely on a system to correct this behavior.”

Advocate

Electronic Petition Filing

We recommend exploring modernization steps implemented by other jurisdictions that allow for the electronic filing of protection order materials (North Carolina Judicial Branch 2019). In communities with electronic filing, survivors can make initial appearances via a video conference with a judge, reducing the need for the survivor to physically appear in court. Making numerous, in-person court appearances can serve to undermine a survivor's safety plan and present additional barriers, such as time off of work and childcare challenges. Additionally, arranging to physically appear in court presents significant barriers to survivors with mobility issues. Elements of such electronic filing systems involve sending email or text message updates to the parties regarding specific proceedings in the case. Electronic petition filing also increases efficiency within the protection order process, as court personnel and judicial officers reduce the amount of time they dedicate to deciphering handwritten petitions.

E-Orders

Research participants recommend adopting E-Orders in Civil Protection Order proceedings. An E-Order system allows judicial officers to generate electronic orders that they review, modify, and sign digitally. Once the judicial officer signs an E-Order, the document is filed with the Clerk's Office. This system allows petitioners and respondents to opt-in for E-Service, which allows parties to immediately receive copies of signed orders by email. E-Orders are already used in other civil and criminal proceedings in King County and research participants indicate that the technology exists to support utilizing an E-Order system within the protection order calendars. Research participants also indicate that this process assists in the enforcement of protection orders, as enforcement officers spend less time deciphering handwritten text.

Consistent and Specific TECC Language in Orders

Participants identified interest in the incorporation of more specific TECC language in protection orders. Specific language assists with clear expectations for all parties, along with providing clear guidelines for enforcement. When the distribution of intimate images is a concern, judicial officers should include specific prohibitions regarding the distribution of intimate images and violations should be taken seriously. We reiterate the importance of training for judicial officers to assist in gaining familiarity with TECC and to encourage the inclusion of appropriately specific, TECC-responsive language in protection orders.

Partner with Tech Companies to Promote Judicial Officer Education

Judicial officers have varying levels of knowledge and familiarity with different technologies and online platforms that survivors and those abusing technology use. In order to close this knowledge gap, we propose targeted partnerships with tech companies to develop written explanatory materials that would be available to all parties. These materials will describe the platform and some of its functionality to provide better context to the court, would be authenticated, and could be filed into the court record by either party. These partnerships will need to be ongoing and nimble as the materials will require updates as platforms evolve and new technologies emerge.

Improve Ability to Consistently Upload Digital Evidence

We recommend exploring an accessible way for survivors to consistently upload digital evidence, including media files, to their protection order petition. Research participants repeatedly referred to inconsistent approaches to document and include this type of evidence for the record. Videos and audio recordings often have tremendous evidentiary value to protection order proceedings and we must develop an accessible way to include such evidence in these hearings.

Commissioners and judges should receive

guidance on how to consider this evidence and incorporate it into the legal record. We appreciate the concerns that some audio or video recordings may have been taken illegally and without consent; judicial officers should not consider such recordings in protection order proceedings. However, survivors are entitled to use such evidence (i.e.: voicemails or video messages) if consent is not an issue.

Electronic Service

While in-person service is the first and optimal choice for protection orders, sometimes it is not possible. Respondents may evade service or be unreachable. Washington's current process allows for secondary methods, with approval from the court, such as service by mail or publication in a newspaper. We recommend stakeholders implement a legislative fix permitting service by email or text message. Especially in situations when the survivor is experiencing device-based harassment, it is more likely that the respondent will receive the information on the device that they are harassing from than service via publication in a newspaper they may never read.

Supply Chain Tracking

Survivors do not currently have access to timely information about the status of the service of their protection order. We support exploring tech-based solutions aligned with supply chain tracking technology to address this issue. Similar to tracking the progress of a package as it moves from shipping to transit to delivery, a supply chain solution to the protection order service process would allow survivors to track the service status of their protection order in real time.

“I would highlight the ease of an abuser’s ability to abuse with technology. It’s so easy for them and the impact is so...the disproportionality between the work they have to do in order to have a very high-level impact.”

Advocate

Conclusions and Next Steps

To conclude this report, we wish to underscore the consistency and uniformity of insight that research participants provided concerning the challenges they experience in supporting survivors of TECC. Regardless of where individual research participants were located or their specific role (as advocates, law enforcement, prosecutors, etc.), each raised overlapping concerns that informed our findings and provided analogous suggestions on recommendations for improvement. This shared understanding of paths forward to better serve survivors who are experiencing TECC and to improve the way our community addresses this issue presents an exciting opportunity to enact broad and meaningful change.

With consistency in appreciation for the scope of the problem and urgency surrounding the necessity for improvement, we encourage stakeholders and decision-makers to take advantage of the current energy and motivation within the community to address the problem of TECC. We hope the findings and recommendations from this report serve as a roadmap for stakeholders and decision-makers to discuss next steps and to implement a strategic plan for how the community will respond to TECC now, and into the future.

References

- Dunlap, Justine. 2012. "Intimate Terrorism and Technology: There's an App for That." *University of Massachusetts Law Review* 7: 10-38.
- Dutton, Mary Ann and Lisa Goodman. 2005. "Coercion in Intimate Partner Violence: Towards a New Conceptualization." *Sex Roles* 52(11/12): 743-756.
- Eaton, Asia, Holly Jacobs and Yanet Ruvalcaba. 2017. "Nationwide Online Study of Nonconsensual Porn Victimization and Perpetration: A Summary Report." Cyber Civil Rights Initiative <https://www.cybercivilrights.org/wp-content/uploads/2017/06/CCRI-2017-Research-Report.pdf>
- Cynthia Fraser, Erica Olsen, Kaofeng Lee, Cindy Southworth and Sarah Tucker. 2010. "The New Age of Stalking: Technological Implications for Stalking." *Juvenile and Family Court Journal* 61(4): 39-55.
- Freed, Diana, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart and Nicola Dell. 2018. "'A Stalker's Paradise': How Intimate Partner Abusers Exploit Technology." *Association for Computing Machinery CHI* April 21–26. <https://doi.org/10.1145/3173574.3174241>
- Goldsworthy, Terry, Matthew Raj and Joseph Crowley. 2017. "'Revenge Porn': An Analysis of Legislative and Policy Responses." *International Journal of Technoethics* 8(2): 26-41.
- Henry, Nicola and Anastasia Powell. 2016. "Sexual Violence in the Digital Age: The Scope of Limits of Criminal Law." *Social and Legal Studies* 25(4): 397-418.
- Kindon, Sara, Rachel Pain and Mike Kesby. 2007. *Participatory Action Research Approaches and Methods: Connecting People, Participation and Place*. New York: Routledge.
- King-Ries, Andrew. 2010. "Teens, Technology, and Cyberstalking: The Domestic Violence Wave of the Future?" *Texas Journal of Women* 20: 131-164.
- McNeal, Ramona S., Susan M Kunkle and Mary Schmeida. 2018. "Defining Online Aggression: From Cyberbullying to Nonconsensual Pornography." IGI Global <https://www.igi-global.com/book/cyber-harassment-policy-reform-digital/187286>
- National Network to End Domestic Violence Safety Net. 2014. *Technology Safety Survey* https://static1.squarespace.com/static/51dc541ce4b03ebab8c5c88c/t/54e3d1b6e4b08500fcb455a0/1424216502058/NNEDV_Glimpse+From+the+Field+-+2014.pdf
- North Carolina Judicial Branch. 2019. "Domestic Violence eFiling System Now Available in Orange County to Increase Victim Safety." *NCCourts.gov* <https://www.nccourts.gov/news/tag/press-release/domestic-violence-efiling-system-now-available-in-orange-county-to-increase-victim-safety> (accessed 1 June 2019)
- Shimizu, Aily. 2013. "Domestic Violence in the Digital Age: Towards the Creation of a Comprehensive Cyberstalking Statute." *Berkeley Journal of Gender, Law & Justice* 28(1): 116-137.
- Cindy Southworth and Sarah Tucker. 2006. "Technology, Stalking and Domestic Violence Victims." *Mississippi Law Journal* 76(1): 667-676.
- Cynthia Southworth, Jerry Finn, Shawndell Dawson, Cynthia Fraser and Sarah Tucker. 2007. "Intimate Partner Violence, Technology, and Stalking." *Violence Against Women* 13(8): 842-856.
- Smith, Linda Tuhiwai. 2005. *Decolonizing Methodologies: Research and Indigenous Peoples*. London: Zed Books.
- Stark, Evan. 2007. *Coercive Control: How Men Entrap Women in Personal Life*. Oxford : Oxford University Press.
- Stoecker, Randy. 2013. *Research Methods for Community Change: A Project-Based Approach* (second edition). Los Angeles: Sage.
- Sweeny, JoAnna. 2017. "Gendered Violence and Victim-Blaming: The Law's Troubling Response to Cyber-Harassment and Revenge Pornography." *International Journal of Technoethics* 8(1): 18-29.
- Tanczer, Leonie, Isabel Lopez Neira, Simon Parkin, Trupti Patel and George Danezis. 2018. "Gender and IoT Research Report: The rise of the Internet of Things and Implications for Technology-facilitated abuse." <https://pdfs.semanticscholar.org/e66f/a45d487285fb322dd5031b31697bb8737f57.pdf>