Legal Evidence of Technology-Facilitated Abuse in Wisconsin: Surfacing Barriers Within and Beyond the Courtroom

SOPHIE STEPHENSON, University of Wisconsin–Madison, USA
NAMAN GUPTA, University of Wisconsin–Madison, USA
AKHIL POLAMARASETTY, University College London, UK
KYLE HUANG, University of Wisconsin–Madison, USA
DAVID YOUSSEF, University of Wisconsin–Madison, USA
KAYLEIGH COWAN, Disability Rights Wisconsin, USA
RAHUL CHATTERJEE, University of Wisconsin–Madison, USA

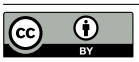
Abusers routinely use technology to spy on and harass their targets. This harmful behavior is known as *technology-facilitated abuse*, or tech abuse. Survivors of tech abuse may turn to the legal system for safety and security, and to do so, they need evidence of tech abuse. However, prior work indicates challenges to collecting evidence of tech abuse and using it in legal proceedings. Thus, in this work, we study legal evidence used by survivors of tech abuse in Wisconsin, USA. We report on qualitative interviews and focus groups with 19 legal support providers who work with survivors seeking protective orders, divorces, and criminal charges. Our findings surface current practices that survivors and legal support providers use to prepare and present evidence of tech abuse in Wisconsin and the challenges they face. For example, survivors struggle to collect evidence of covert monitoring and surveillance. When they can collect evidence, it is often difficult to connect that evidence to the abuser due to the anonymous nature of many forms of tech abuse. In court, evidence of tech abuse is frequently challenged and vulnerable to objections and counter-evidence. And at the end of a proceeding, it's not uncommon for a judge to determine that the tech abuse does not meet the statutes. Informed by these results, we encourage CSCW and HCI researchers to work towards designing and deploying sociotechnical solutions that support survivors' use of evidence, in careful collaboration with advocates, legal experts, and survivors.

CCS Concepts: • **Human-centered computing** → *Empirical studies in HCI*; *Collaborative and social computing*; • **Security and privacy** → *Human and societal aspects of security and privacy*.

Additional Key Words and Phrases: technology-facilitated abuse, digital safety, at-risk users

ACM Reference Format:
Sophie Stephenson, Naman Gupta, Akhil Polamarasetty, Kyle Huang, David Youssef, Kayleigh Cowan, and Rahul Chatterjee. 2025. Legal Evidence of Technology-Facilitated Abuse in Wisconsin: Surfacing Barriers Within and Beyond the Courtroom. *Proc. ACM Hum.-Comput. Interact.* 9, 7, Article CSCW441 (November 2025), 32 pages. https://doi.org/10.1145/3757622

Authors' Contact Information: Sophie Stephenson, sophie.stephenson@cs.wisc.edu, School of Computer, Data & Information Sciences, University of Wisconsin–Madison, Madison, Wisconsin, USA; Naman Gupta, n@cs.wisc.edu, School of Computer, Data & Information Sciences, University of Wisconsin–Madison, Madison, Wisconsin, USA; Akhil Polamarasetty, akhil.polamarasetty.23@ucl.ac.uk, University College London, London, UK; Kyle Huang, kkhuang@wisc.edu, University of Wisconsin–Madison, Madison, Wisconsin, USA; David Youssef, dyoussef@wisc.edu, University of Wisconsin–Madison, Madison, Wisconsin, USA; Kayleigh Cowan, kayleighc@drwi.org, Disability Rights Wisconsin, Madison, Wisconsin, USA; Rahul Chatterjee, rahul.chatterjee@wisc.edu, Computer Science, University of Wisconsin–Madison, Madison, Wisconsin, USA.



ACM 2573-0142/2025/11-ARTCSCW441
https://doi.org/10.1145/3757622

Content warning: *This paper contains descriptions of abusive behavior, often in the context of intimate partner violence, that may be difficult to read.*

1 Introduction

Technology-facilitated abuse, also known as tech abuse, is a growing problem globally [48, 49, 56, 58, 61, 74, 84, 85, 118]. Abusive intimate partners, family members, and others frequently use technology against their targets—in one study, for example, 80% of stalking survivors reported being stalked with technology [105]. Tech abuse can violate a survivor's privacy, isolate them from support systems [65, 84], and sometimes foreshadow physical and sexual violence [62].

Survivors of tech abuse often turn to the legal system for physical and digital safety and security by, e.g., filing for a restraining order or seeking criminal charges [61, 65]. To procure these legal protections, survivors need to provide evidence of tech abuse. Unfortunately, they face multiple challenges to using evidence of tech abuse in legal proceedings [39, 61, 68, 107, 120]. For example, the onus is on the survivor to "tie the digital abuse to offenses that are recognized by the law" [61]. Doing so is a burden for survivors, who must provide a great deal of context so that others can understand the harms of the abuse [65]. In addition, legal professionals have been known to minimize the severity of tech abuse, seeing it as not "real" compared to physical abuse, or otherwise may lack knowledge of tech abuse and its harms [44, 61, 65, 107].

The aforementioned challenges are concerning for survivors, yet much remains unknown about how survivors prepare and present legal evidence of tech abuse and the challenges they face when doing so. Thus, in this work, we conducted a qualitative study with 19 support providers who help survivors use evidence of tech abuse in U.S. legal proceedings. Since U.S. states use differing legal statutes and procedures, we focused on evidence of tech abuse in legal proceedings of a single state—Wisconsin—enabling us to hone in on survivors' needs in this context. Our research questions are as follows:

RQ1: How do survivors in Wisconsin prepare and present legal evidence of tech abuse?
RQ2: What challenges do survivors face when attempting to use evidence of tech abuse in Wisconsin legal proceedings?

We conducted interviews and focus groups with 19 legal support providers, including advocates, attorneys, and law enforcement, who have supported survivors in preparing and presenting evidence of tech abuse in Wisconsin legal proceedings. Primarily, the support providers discussed cases where tech abuse occurred in the context of intimate partner violence.

First, we identified many types of evidence of tech abuse used in practice (Section 4). The legal support providers have seen evidence used to prove four broad types of tech abuse: harassment & intimidation, monitoring & surveillance, image-based sexual abuse (IBSA), and financial abuse. Much of the evidence they've observed captures abusive acts themselves using, typically, screenshots of harassing messages, defaming posts, impersonated actions, or non-consensual images. Logs from platforms or cell providers add extra argumentative weight. On the other hand, some types of tech abuse—especially covert monitoring and surveillance—are harder to document. Detailed account logs, if available, can show when an abuser views private data. Otherwise, survivors bring in a spy device they found surveilling them, screenshot proof that an abuser had the *ability* to monitor them, or rely on circumstantial evidence.

In tandem, we surface 25 challenges that survivors face while preparing (Section 5) and presenting (Section 6) legal evidence of tech abuse. For example, survivors must provide all evidence necessary to give context and demonstrate the harms, but also prioritize only the most legally relevant evidence to avoid overwhelming court decisionmakers with *too much* evidence. At the same time, evidence of tech abuse is sometimes scarce—many surveilling behaviors, for example, leave little

trace. Once in court, high authentication standards are applied to the evidence, making it easier for abusers to cast doubt on its veracity with forged counter-evidence. In the end, there are many times when tech abuse is not determined to be illegal because it doesn't quite fit the legal statutes.

Our results indicate several opportunities for CSCW researchers and technologists to support survivors through platform changes and carefully-designed socio-technical tools (Section 7). Technologists should increase the transparency of digital technologies with detailed activity logs to augment the available evidence of surveillance while being careful not to provide another vector for surveillance. Researchers, in tandem, should design tools that help survivors identify, capture, prioritize, and format evidence in accordance with legal standards. Tools like this would reduce survivors' burden and could potentially be integrated into existing interventions. The HCI community must engage with advocates, survivors, and legal stakeholders to ensure that these resources protect survivor safety and are effective in practice.

2 Background & Related Work

In this section, we review technology-facilitated abuse (or tech abuse, Section 2.1); tech abuse in intimate partner violence (IPV), the most common context discussed in our study (Section 2.2); challenges to legal mitigations for tech abuse (Section 2.3); and relevant Wisconsin legal background (Section 2.4).

2.1 Technology-Facilitated Abuse

Early works including Dimond et al. [48], Matthews et al. [84], Woodlock [118], and Freed et al. [61] identified that abusive intimate partners, family members, and others routinely use technology to stalk, harass, dox, and spy on their partners. This pattern is called technology-facilitated abuse, or tech abuse for short. In recent years, researchers have identified many harmful forms of tech abuse. Abusers use tailored spyware apps [23, 98], "dual-use" [37] applications, access to online accounts [28, 61], and physical spy devices [35, 73] to facilitate monitoring and surveillance. In addition, abusers use technology to harass survivors in numerous ways, including through messages [60, 109], social media posts [60], online impersonation [84], blocking access to technology [79], manipulating smart home devices [80, 89, 103, 107, 108, 110], or financial abuse and coerced debt [22, 26, 27, 30]. Tech abuse also includes image-based sexual abuse (IBSA), where abusers capture, keep, (threaten to) share, or even AI-generate [32] intimate images without consent [24, 74, 74–77, 91, 92]. Broadly, Freed et al. described abusers as *UI-bound adversaries* [60] who use unsophisticated methods to enact tech abuse, combined with psychological coercion, intimate knowledge of the survivor, and physical access to devices [112].

Tech abuse is a grave concern for survivors. It can violate survivors' privacy, isolate them from support systems [65, 84], foreshadow physical, psychological, or sexual violence [62], or threaten the life or safety of survivors' friends, family, or pets [65, 108]. Tech abuse is an increasingly prevalent occurrence in the U.S. [58, 60, 84] and globally [88]; for example, recent studies show 70-80% of stalking survivors reported that the stalker used technology [64, 105].

2.2 Tech Abuse in Intimate Partner Violence

Tech abuse occurs in many contexts, but due to the expertise of the support providers we interviewed, this paper is primarily about tech abuse within intimate partner violence. IPV is defined as "physical, sexual, or psychological harm by a current or former intimate partner or spouse" [10]. One in three women globally [9] face IPV during their lifetime. Women [9, 104], people of color [97], and the LGBTQ+ community [38] are disproportionately affected by IPV.

Intimate abusers are known to use *coercive control* [106] tactics encompassing not only physical and sexual abuse, but emotional and psychological torment. Coercive control tactics are highly

personalized and contextual to the relationship between the survivor and abusive partner [106]. Today, technology plays a large role in this coercive control, with some scholars referring to tech abuse in IPV as "digital coercive control" [67, 69] or "technology-facilitated coercive control" [40, 41, 44, 50, 51]. Indeed, Cuomo and Dolci have argued that tech abuse is "a continuation of harm … rather than a new or distinct form of abuse" [44, p. 224], emphasizing that abusers use new technological tools to enact existing coercive control tactics. Supporting this argument, prior work from Duerksen and Woodin [52] showed that in-person IPV perpetration is a predictor for technology-facilitated coercive control in IPV.

2.2.1 IPV tech clinics. Although survivors of tech abuse in IPV seek support from their friends and family [34, 64, 65] or victim service providers, HCI researchers have recently designed a *clinical computer security model* [71] that can provide more tailored technological support. In this model, trained technologists provide tailored, one-on-one support to IPV survivors. These consultants search for indications of tech abuse manually and using automated scanning tools, then advise the client on securing their digital assets. To date, three *tech clinics* in the U.S. offer these consultations: the Clinic to End Tech Abuse (CETA) [5], the Technology-Enabled Coercive Control (TECC) Clinic [40, 42, 45], and the Madison Tech Clinic [19]. In recent years, there has been much research to understand the role of tech clinics and improve their service model [43, 59, 95, 113–115].

2.3 Barriers to Legal Action Against Tech Abuse

Whether tech abuse occurs in the context of IPV or other forms of abuse, survivors often turn to informal and formal interventions to mitigate abuse and seek protective actions [65, 68, 120]. One often-sought intervention is legal action through the criminal justice system. Legal action is possible because, in many cases, tech abuse is illegal. For example, technology-facilitated stalking is prohibited in every U.S. jurisdiction [105]. Douglas et al. [49] illustrated some examples of successful legal action in practice, such as survivors adding technology-related conditions to orders of protection. However, prior work in fields such as HCI, criminology, and feminist geography has identified several barriers to legal action against tech abuse that add to survivors' burden of "advocating for themselves to police, lawyers, and judges" [33, p. 13].

2.3.1 Victim-blaming and disenfranchisement. To begin, survivors of tech abuse face several systemic issues present in the legal response to violence survivors. Marginalized survivors face discrimination, racism, and sexism [57, 64, 78, 119], especially during legal interventions [78, 120]. For example, Indigenous women [33, 81] and Muslim survivors [93, 94] face additional challenges interacting with the legal system due to cultural and language barriers, a lack of available services, and tension between the federal government and Indigenous sovereignty [33, 81, 117]. Specific to IPV, Cuomo and Dolci eloquently argued that "patriarchy and institutionalized sexism situate domestic violence and survivors' needs for protection as secondary to the convenience of maintaining a traditional legal system" [46, p. 920]. These biases, combined with rampant victim-blaming in the criminal justice system, leave survivors feeling disenfranchised grief and institutional betrayal [68, 120].

2.3.2 Challenges identifying tech abuse. Specific to tech abuse, the first challenge survivors may have is identifying tech abuse in the first place. The "invisible" [61] nature of tech abuse makes it challenging to know tech abuse is occurring, let alone seek support [65] or take legal action [61]. Citron et al. [39] highlighted that "people cannot seek redress for harms they don't know about"—if a survivor cannot find any concrete evidence that they are being surveilled using technology, then they cannot seek action against those harms. Unfortunately, it is common for survivors to know they are being surveilled, but not know how the surveillance is being perpetrated [61].

2.3.3 Challenges capturing evidence. Evidence of tech abuse is the focus of this work, given its importance in taking legal action. Securing evidence can be difficult for survivors. It isn't always clear *which* evidence should be collected or *how* to collect it. Online guides offer some help, but are missing practical details—e.g., the Safety Net Project recommends documenting "only relevant information" [3], but what is relevant may depend on (a) the context of the abuse and (b) the specific legal statutes related to the survivor's proceeding. Furthermore, evidence collection is not explicitly offered by the tech clinics, and, at the time of writing, one (Madison Tech Clinic) cautions survivors against relying on the clinic for evidence collection [19]. Finally, the presence of abusers can make preparing evidence dangerous for survivors and, once it is collected, abusers could delete the evidence if they know where it is stored [61].

Further challenges exist when collecting online data. It can be hard for survivors to communicate with technology platforms to collect evidence, especially if it's already been taken down [61, 102]. Scholars such as Freed et al. [61] and Slupska and Strohmayer [102] have argued that technology platforms face the tension of content moderation versus retaining useful information as evidence that survivors can use. There can also be complications due to anonymity or ownership issues. For example, abusers often anonymize themselves by cycling phone numbers or creating new online accounts [39, 61, 102].

2.3.4 Challenges presenting evidence. Even when survivors can collect evidence, it is often ignored, which can result in institutional betrayal and disenfranchisement as criminal justice professionals question the relevance of tech abuse [65, 70, 102]. For example, Powell and Henry's Australia-based study [90] showed that law enforcement often treat tech abuse as separate from, and less harmful than, other forms of abuse. In some cases, evidence of tech abuse is even used against survivors—e.g., recordings showing that the abuser was spying with hidden cameras could be manipulated to show only parts that suit the perpetrator's case [102]. Regehr et al. [96] and Stephenson et al. [109] also pointed out that digital evidence often persists against survivors' wishes, potentially re-traumatizing them.

2.3.5 Gaps in legislation. Although there are legal options for survivors, legal recourse for tech abuse may be limited or nonexistent [61]. For example, it is not always clear whether surveillance through smart home or Internet of Things (IoT) devices fits into statutes for restraining orders [107]. Similarly, some laws against IBSA only consider public distribution, making it legal to share the content directly with others [39]. Ownership of IBSA material and other digital content is opaque in both laws and social norms [54, 55, 82, 87]. Some laws require survivors to prove that the abuser's intention was malicious, which may be obvious to the survivor but difficult to prove concretely [39]. Overall, survivors may struggle with knowing how and where to report tech abuse [70, 120].

In an attempt to close these gaps, new proposals include provisions to protect against abuse involving smart devices [7, 8], misuse of survivors' personal information online [6, 11], and creation of deepfake IBSA [63]. The Safe Connections Act of 2022 [12] allows survivors to separate their phone plan from a shared family plan, often managed by the abuser [83]. However, U.S. law still lags behind technology, neglecting to recognize many varieties of tech abuse.

Our work complements prior research by focusing on how survivors use evidence of tech abuse in Wisconsin legal proceedings. We aim to understand the breadth of evidence of tech abuse used in practice, the strategies for preparing and presenting evidence of tech abuse, and the challenges that survivors and their legal support providers face during the process.

Table 1. Background information on the three broad types of proceedings most relevant to this research: restraining orders, divorces, and criminal charges. When multiple decisionmakers are listed, the first person or group makes the final decision, and the rest (in parentheses) make intermediate decisions. For example, in criminal proceedings, the jury decides guilt, but the judge admits evidence.

	Restraining Order	**Divorce**	**Criminal Charges**
Court type	Civil	Family	Criminal
Survivor's role	Petitioner	Petitioner	Victim
Abuser's role	Respondent	Respondent or joint petitioner	Defendant
Decisionmaker	Judge	Judge (GAL†)	Jury (Judge)
Burden of proof	Preponderance*	Preponderance*	Beyond a reasonable doubt
Survior's goal	A protective order barring the abuser from contact; Possibly additional protective orders specific to tech abuse.	A preferred custody & placement decision; Possibly additional protective orders specific to tech abuse.	Legal punishment; Financial reimbursement; Jail time for the abuser (i.e., physical safety).

†GAL = Guardian Ad Litem *Preponderance = More likely than not

2.4 Wisconsin Legal Background

This study focuses specifically on legal evidence of tech abuse in Wisconsin. In Wisconsin, the legal actions most relevant to tech abuse are restraining orders, divorces, and criminal charges (Table 1). Table 5 in the Appendix discusses more about the specific Wisconsin statutes most relevant to this study.

2.4.1 Key definitions: Stalking, harassment, and domestic abuse. Many legal actions for tech abuse in Wisconsin are built upon legal definitions of harassment and stalking. Per WI §947.013, harassment is briefly defined as either physical violence or "repeatedly commit[ting] acts which harass or intimidate the person and which serve no legitimate purpose," making it potentially applicable to several forms of tech abuse. Stalking (WI §940.32) is defined as a course of conduct—potentially including technology-facilitated monitoring, recording, or contact—that (i) would cause a reasonable person distress or fear of bodily injury, (ii) is intended to cause distress or fear, and (iii) does cause that distress or fear. Notably, the legal definition of domestic abuse (WI §968.075) refers only to physical or sexual violence, making it irrelevant to tech abuse.

2.4.2 Restraining orders. When granted, restraining orders (ROs) bar the abuser (the *respondent*) from contacting or approaching the survivor (the *petitioner*). In Wisconsin, survivors typically make use of one of two types of ROs: domestic abuse (WI §813.12) and harassment (WI §813.125). Domestic abuse ROs concern physical or sexual abuse, property damage, and stalking;[1] harassment ROs concern physical or sexual abuse, stalking, and harassment. Violating an RO can result in criminal charges.

To get an RO, the survivor files a petition with the court. Then, the court may grant a temporary restraining order (TRO) that bars the abuser from contact with the survivor leading up to the civil *injunction hearing*, which is scheduled approximately two weeks after filing. At the injunction hearing, a judge hears arguments from both the petitioner and the respondent and may grant the full RO, which can last between 2 and 10 years. The petitioner must show *preponderance of the*

[1]Note that the domestic abuse RO statute (WI §813.12) is relevant to tech abuse, while the broad domestic abuse statute (WI §968.075) is not. This important nuance adds to the challenges survivors face when trying to present evidence of tech abuse (Section 6).

evidence: greater than a 50% chance that the respondent violated the RO statutes. Oftentimes, RO petitioners are *pro se*, meaning they represent themselves [18].

2.4.3 Divorce. Survivors may be married to and/or co-parent children with their abusers. Legally, divorce proceedings are required to take any domestic abuse into account for child custody and placement decisions (WI §767.405(14)(a)2m), although this is not always the case in practice [86]. It is also possible for survivors to request ad hoc protective orders during these proceedings based on evidence of abuse; for example, a requirement that the abuser refrain from using location trackers to monitor the survivor. Decisions are made by a judge, but sometimes a Guardian ad Litem (GAL) is also assigned to give their opinion on custody & placement decisions with the goal of supporting the best interests of the children.

2.4.4 Criminal law. Finally, there are many potential criminal charges against abusers. The broadest and most relevant are stalking and harassment, mentioned above. Human trafficking (WI §940.302) is another broad statute which, while only applicable to trafficking cases, covers acts like coercion, threats, and intimidation for which traffickers often leverage technology [109]. Other potential criminal charges include: global positioning devices (WI §940.315), which prohibits using GPS devices to track someone without consent; defamation (WI §942.01); invasion of privacy (WI §942.08), which prohibits spying on someone with the intent to watch them nude; and representations depicting nudity (WI §942.09), which prohibits the capture, reproduction, possession, or distribution of an intimate representation without consent. Several other statutes are detailed in Table 5 in the Appendix.

Criminal proceedings are handled by state prosecution on behalf of the survivor. By law, the prosecution must prove beyond a reasonable doubt that the crime occurred.

2.4.5 Evidence admissibility rules. Survivors use evidence of tech abuse to support their legal arguments. To do so, the evidence must be admitted in court. The Wisconsin Rules of Evidence are fairly straightforward.[2] The primary requirement is simply "evidence sufficient to support a finding that the matter in question is what its proponent claims" (WI §909.01). Additionally, evidence must be *relevant*, meaning it must make the existence of any fact that is of consequence to the determination of the action more or less probable than it would be without the evidence (WI §904.02). As we'll discuss, this means the evidence must be tied to both the abuser and the survivor. Even if relevant, evidence may be excluded if its probative value is substantially outweighed by a danger of unfair prejudice, such as biasing or confusing the decision maker (WI §904.03). Hearsay (essentially, something one of the parties said outside of court) is generally not allowed (WI §908.02), although there are many exceptions to the rule.

There are few special requirements for admitting digital evidence. In fact, historical precedent regarding WI §909.01 specifies that "Text and other electronic messages do not require new rules on authentication." The statutes specify that any photos submitted as evidence must be an "original" document, which includes screenshots (WI §910.02).

3 Method

To better understand how legal evidence of tech abuse is used in practice, we conducted a qualitative study focusing on Wisconsin legal proceedings. We bounded our study to Wisconsin to surface patterns in how evidence of tech abuse is used in legal contexts, and any challenges to using evidence of tech abuse, without the complexity of considering legal contexts in other U.S. states.

Session procedures are provided in a public GitHub repository.[3]

[2]There are also federal rules of evidence, but we omit them here as they do not apply to state courts.
[3]https://github.com/WISPR-lab/CSCW2025-Evidence-Supplementary

3.1 Positionality, Ethics, and Research Justice

3.1.1 Positionality statement. We embrace a reflexive approach to qualitative research, acknowledging that our ways of seeing impact the outcome of the study [31, 72]. One author is an attorney representing IPV survivors in both civil and criminal contexts, who helped us shape the study, analysis, and writing to accurately reflect the Wisconsin legal landscape. All other authors volunteer with Madison Tech Clinic, which provides direct trauma-informed support services to survivors of tech abuse in IPV in Wisconsin. We frequently get requests from survivors to support them with evidence collection, and we have observed the challenges survivors face when making evidentiary requests. Furthermore, some authors have personal experience with IPV that further grounded our methodology with a survivor-oriented lens.[4] Like many of the legal support providers we spoke with, the interviewer is a white woman from Wisconsin. The authors used trauma-informed principles of care [4] while conducting sessions and analyzing the data.

3.1.2 Ethical considerations. Our research was approved by the university's ethics review board. Given the sensitivity of legal support providers' work, we took additional steps to guarantee the safety and confidentiality of the legal support providers and the survivors they support (their *clients*). We used many of the strategies outlined by Bellini et al. [29] in their survey of research on at-risk users. Most notably, we used legal support providers as *proxies* for this research instead of directly interviewing survivors in order to prevent re-traumatization. Legal support providers could decline audio recording for their interview, although none chose this option. We asked support providers not to share identifying information about any of their clients during the sessions, and they diligently followed this advice. In addition, transcripts were fully anonymized before being stored in a secure repository, and raw recordings were destroyed as soon as transcripts were created. Finally, throughout the study, we sought advice from legal advocates, attorneys, and other partners familiar with the evidence of tech abuse, one of whom is a co-author of this paper, for ecological validity.

3.1.3 Research justice. We are dedicated to research justice and will take steps to ensure that this work positively benefits survivors and their advocates. We plan to use the findings from this work to design an evidence-collection tool that survivors can use in Madison Tech Clinic consultations. In the meantime, we commit to sharing our findings with the legal support providers, our partner organizations, and others in Wisconsin who may benefit from seeing our results. For example, in collaboration with the Wisconsin Office of Court Operations, we are facilitating trainings for judges based on this study. Finally, we will carefully evaluate the final academic publication to ensure that it will not cause harm to the legal support providers, their clients, or survivors generally after publication.

3.2 Semi-Structured Interviews & Focus Groups

We conducted semi-structured focus groups and interviews (collectively, "sessions") with 19 legal support providers (P01–P19). We did not interview survivors directly to avoid retraumatization and to protect their safety and privacy, as they may be actively involved in legal actions [29].

3.2.1 Session types. In victim service providers and law clinics, legal support providers commonly discuss their cases amongst co-workers to get support and share best practices. We know this from our experience working with providers as part of Madison Tech Clinic. Since the work is so often

[4]We want to assert that although the authors here chose to disclose lived experience, such disclosure should always be optional and at the discretion of those with the lived experience. Furthermore, we emphasize that lived experience is not a requirement when doing research about IPV, nor is experience providing direct survivor support.

Table 2. Aggregate demographics for the 19 legal support providers who participated in the study. Legal support providers may fall into multiple categories for roles and race/ethnicity. One attorney did not fill out our demographic form.

Role		Years of Advocacy		Age		Gender		Race/Ethnicity	
Program lead	8	<2 years	6	18-24 years	3	Woman	16	White	16
Legal advocate	5	2-5 years	5	25-34 years	6	Man	2	Asian	2
Attorney	4	6-9 years	1	35-44 years	5			Black or African American	1
Law clinician	4	10+ years	6	45-54 years	2				
Judge	1			55-64 years	2				
Police officer	1								
SANE†	1								

†SANE = Sexual Assault Nurse Examiner

collaborative, we gave legal support providers the option to be interviewed alone or to participate in a collaborative setting with their co-workers.

Out of the 19 legal support providers, 10 providers from 3 organizations chose the focus group option, while 9 providers opted for an individual interview. Thus, we held 3 focus groups and 9 individual interviews for a total of 12 sessions. We held 2 in-person focus groups and ran the rest of the sessions over Zoom.

3.2.2 Recruitment. We recruited the legal support providers through direct emails and phone calls, using prior connections or contact information shared on organization websites. We also posted fliers in places like the county courthouse, local victim service providers, and other public places frequented by legal experts. Furthermore, we advertised the study on relevant email lists run by a statewide IPV advocacy agency. The legal support providers were offered $20 USD per hour as compensation; four declined payment.

To participate in the study, legal support providers had to be (i) at least 18 years old, (ii) living and working in Wisconsin, and (iii) have experience collecting, presenting, or adjudicating evidence of tech abuse for legal proceedings, or supporting survivors with those tasks.

3.2.3 Session procedures. We used the following procedure for all sessions, allowing one hour for individual interviews and two hours for focus groups. To begin, we shared the consent form and asked for verbal informed consent to participate in the study and, optionally, to audio-record the session. All legal support providers consented to record. We began with warm-up questions about the providers' roles and the tech abuse faced by their clients. Then, we asked about the types of evidence of tech abuse they have seen in practice, the process for collecting and presenting evidence of tech abuse, and what makes evidence work in their experience. In early interviews, we sought feedback from the legal support providers and adjusted the protocol as necessary. For example, we tweaked the wording and added a question specifically about the types of tech abuse we commonly see in Madison Tech Clinic, like account compromise.

3.2.4 Data preparation. We created an anonymized transcript of each session, using Otter.ai to generate an initial transcript. The first author listened to each recording, fixed errors, and redacted references to potentially identifying information: usually, the support provider's name, names of their colleagues, their organization, or their location. As soon as the transcript was cleaned and anonymized, we deleted the audio recording from our local machine and the Otter.ai server.

3.3 Participating Legal Support Providers

The 19 legal support providers held a variety of roles (Table 2). They included 5 legal advocates (people who provide legal guidance at a victim service provider), 5 program directors, 4 attorneys, 2 law students who volunteer at a restraining order clinic, a police officer, a judge, and a sexual assault nurse examiner (SANE). Some providers—a legal advocate, an attorney, and the SANE—also hold leadership positions in their programs. The 5 program directors all have direct service experience in addition to overseeing advocates and their clients, meaning they shared about the cases they have personally managed and broad trends they've observed at their victim service provider. The SANE has previously served as an expert witness and sees evidence of tech abuse used while providing support to her clients.

The legal support providers work in nine counties of Wisconsin at twelve different organizations. Three were from the statewide IPV advocacy organization that helped us advertise the study. The majority of the legal support providers are white women.

3.4 Data Analysis Procedure

We analyzed the interview data inductively via Kuckartz's thematic qualitative text analysis methodology [2]. After initial familiarization with the text, our coding process had three stages.

In stage one, we aimed to generate high-level thematic categories and apply them to our dataset. To begin this phase, the first, second, and third authors (the *primary coders*) independently coded one session and developed individual codebooks. We met to discuss our experiences coding, share our individual codebooks, and agree on an initial, shared codebook with six high-level categories. Next, the primary coders independently coded two additional sessions using this shared codebook, then met to solidify any necessary changes or additions to the codebook.

After creating high-level themes, the fourth and fifth authors (the *secondary coders*) joined the analysis process to help distribute the workload. The first author met with the secondary coders to explain the codebook and how to apply it. Then, the primary and secondary coders coded all data, including session transcripts, session notes, and researcher memos. All data was double-coded, and at least one primary coder coded each piece of data.

In stage two, the first author looked at all text coded within each higher-level category and generated sub-categories. For instance, for the category "tech abuse captured in evidence," she generated subcategories such as "harassing messages and calls" or "location tracking." The first author then re-coded the data using these new, more detailed subcategories, consulting with other authors regarding any confusion.

The third and final stage involved a category-based analysis of the results. The first author analyzed across categories and subcategories to understand the connections between ideas, then met with the other authors to discuss these findings. For example, she looked at the challenges of presenting evidence in different legal contexts and with different forms of evidence. She also compared the different types of legal support providers (broadly: legal representation, advocates who do not provide representation, and law enforcement), finding that the themes were largely consistent across the three groups.

3.5 Limitations

Like most qualitative studies, the study may have self-selection bias. People who chose to participate likely have more interest in the topic or hold stronger opinions about it. Judges or police officers who signed up have some awareness of tech abuse, which, as we saw in our findings, is not always the case. Additionally, it's possible that the support providers recalled information incorrectly or spoke about colleagues' cases without knowing all the facts of the case.

Table 3. We detail the codes we generated about different types of evidence of tech abuse the legal support providers described. Evidence most commonly captured evidence of harassment (especially harassing messages and calls), location tracking, and account compromise. Typically, evidence consists of photos & screenshots, testimony, and account logs & statements.

Category	Code	# References	# Sessions
Tech Abuse Captured	Harassment & intimidation	130	12 (100%)
	↪ *Harassment over messages or calls*	*99*	*11 (92%)*
	↪ *Harassment on social media*	*17*	*6 (50%)*
	↪ *Device compromise or control*	*11*	*3 (21%)*
	↪ *Online impersonation*	*3*	*3 (21%)*
	Monitoring & surveillance	66	7 (58%)
	↪ *Location tracking*	*44*	*7 (58%)*
	↪ *Account compromise*	*20*	*6 (50%)*
	↪ *Surveillance with recording devices*	*19*	*4 (33%)*
	↪ *Spyware*	*3*	*2 (13%)*
	Image-based sexual abuse (IBSA)	26	6 (50%)
	Financial abuse	3	2 (13%)
Evidence Types	Photos & screenshots	95	12 (100%)
	Testimony	62	8 (67%)
	Account logs & statements	44	9 (75%)
	Audio	25	7 (58%)
	Physical device	21	8 (67%)
	Cell data	7	3 (21%)
	Prior police reports	6	3 (21%)
	Ankle monitor data	2	2 (13%)
	IP activity	2	2 (13%)
	Tech clinic summary	1	1 (8%)
Evidence Formats	Printed out	21	6 (50%)
	Digitally stored	20	7 (58%)
	Shown on phone	5	2 (13%)

The demographic makeup of the legal support providers presents other limitations. As previously stated, we used proxies instead of interviewing survivors directly, meaning we did not hear the first-hand lived experiences of any survivors. The providers are also overwhelmingly white women and based in more urban counties of Wisconsin. The demographic breakdown is unsurprising given that most survivor advocates are women [20] and considering the demographics of Wisconsin [1], but also ignores the marginalization of people of color who face tech abuse and IPV at a much higher rate (e.g., [97]). Therefore, when it is beneficial and appropriate to do so, future work should seek to understand the challenges faced by survivors of color.

Finally, our study is only relevant to survivors who wish to interact with the U.S. legal system. Many survivors avoid legal action due to a number of factors, such as cost, time, and disenfranchisement from law enforcement [65, 120]. Since we limit the focus of our paper to Wisconsin legal proceedings, however, we believe that future studies could explore evidence practices in non-western judicial contexts, building upon prior work in South Asia [25, 99, 100].

4 Evidence of Tech Abuse in Practice

From our interviews with legal support providers, we identified many varieties of evidence of tech abuse that are used in practice. Table 3 summarizes the types of evidence.

4.1 Types of Tech Abuse Mentioned

The legal support providers have observed evidence capturing four broad categories of tech abuse (Table 3): technology-facilitated (i) harassment & intimidation, (ii) monitoring & surveillance, (iii) IBSA, and (iv) financial abuse. These types of tech abuse may match a number of Wisconsin statutes—or none at all—depending on the situation. E.g., tech abuse falling under *harassment & intimidation* would be covered under the harassment statutes, but potentially also other statutes such as defamation. See Table 5 for more details on the specific statutes.

There are other forms of tech abuse that the legal support providers have *not* observed in legal proceedings—for example, abuse involving smart home devices. This omission may reflect a lack of evidence of this type of abuse (Section 5.1) or indicate that these additional forms of tech abuse do not fit Wisconsin statutes (Section 6.3).

4.1.1 Harassment & intimidation. These concerns were brought up in every session. The legal support providers have most often seen evidence of harassment and intimidation through direct messages and calls. Less commonly, they have also observed evidence of public harassment on social media and impersonation through a survivor's online accounts (e.g., un-enrolling them from university).

4.1.2 Monitoring & surveillance. Being spied on is a common concern for survivors, and accordingly, evidence of monitoring and surveillance came up in over half of our sessions. The legal support providers have most often seen evidence of location tracking, but have also observed evidence of surveillance with recording devices (e.g., cameras and audio recorders) and surveillance of online accounts. Although uncommon, evidence of monitoring via spyware apps was also mentioned.

4.1.3 Image-based sexual abuse (IBSA). IBSA came up in half of the sessions. The providers mentioned that abusers capture intimate images without consent and distribute them privately or publicly. They also discussed how abusers might threaten to share intimate imagery as a form of control, regardless of whether they actually distribute the images.

4.1.4 Financial abuse. Finally, technology-facilitated financial abuse [26] came up a few times. Providers mentioned that abusers use access to joint financial accounts, or to the survivor's personal financial account, to steal funds.

4.1.5 Legal context. Legal support providers have seen evidence of these kinds of tech abuse primarily in Wisconsin restraining order injunctions and violations, family law, and criminal proceedings. A few providers mentioned tort law and national immigration law under the Violence Against Women Act (VAWA) [21]. Although immigration law can be crucial for some survivors, we focus on Wisconsin civil, family, and criminal proceedings to keep scope to Wisconsin and focus on the most frequently-mentioned legal contexts. To provide more detailed legal context, Table 5 in the Appendix maps relevant Wisconsin statutes to the four types of tech abuse that came up.

4.2 Types of Evidence Used to Prove Tech Abuse

In practice, evidence of tech abuse comes in a variety of forms, ranging from printed photos & screenshots to physical surveillance devices. We found three broad groups of evidence of tech abuse: evidence capturing an abusive act, evidence that connects the abuser to these abusive acts, and circumstantial evidence of tech abuse. The providers reported that testimony is a foundational type of evidence that they see used to prove all kinds of tech abuse—albeit not without challenges (Section 6.2).

4.2.1 Evidence capturing the abusive act itself. Many forms of tech abuse, such as harassing messages or the use of spyware apps, leave a trace online or on survivors' devices. Accordingly, those abusive acts can potentially be captured as evidence. Survivors use photos & screenshots to capture messages, social media posts, impersonated activity, or intimate images. The same information can also be captured with records from phone providers, social media platforms, or financial institutions. To capture harassing phone calls, survivors sometimes audio record the call or take a screenshot showing the number of calls they have received. The legal support providers have also observed survivors submitting the abuser's device as evidence, showing that IBSA material is present on the device.

Evidence of monitoring and surveillance is less readily available, since these behaviors are often covert. The most concrete evidence of monitoring is the presence of physical surveillance devices: for example, an AirTag found on a survivor's car, or a camera discovered in the survivor's home. The devices themselves, photos of the devices, or data captured from surveillance devices (such as location data or recorded videos) are all used as evidence. In a similar vein, one support provider recalled using an expert witness, a forensic investigator, who testified that they had found spyware on the client's device. However, forensic investigators may not be available to all survivors (Section 5.3).

When monitoring instead occurs via accounts—a common concern [61]—survivors sometimes use detailed account logs (e.g., on an Amazon Alexa) to show what data an abuser viewed and when. One legal support provider also recalled that a client got evidence from the manufacturer of their car which showed that the abuser had set up tracking alerts for the car's location. Survivors also show that their account was accessed from an unfamiliar IP address.

4.2.2 Evidence connecting the abuser to the tech abuse. Survivors need to prove that the abuser was the person doing the abusive behaviors. They prove this by demonstrating the abuser's ownership of a harassing phone number, IP addresses associated with abusive behavior, and abusive online personas. Sometimes, survivors can show that the abuser has previously posted similar content under their own name.

4.2.3 Circumstantial evidence of tech abuse. In many cases, it is not possible to concretely show that tech abuse has occurred. Survivors in these situations sometimes show that an abuser previously talked about enacting tech abuse—for instance, by taking screenshots of an abuser's message that talks about distributing IBSA material. They might also provide evidence showing that an abuser, e.g., purchased a GPS device, or searched for surveillance devices online.

A common type of circumstantial evidence is evidence that an abuser had the *ability* to surveil a survivor online, without being able to prove that the abuser *used* that capability. For example, survivors show (typically using a screenshot) that their abuser has access to their location via Apple FindMy or that the abuser's device is connected to their account. One legal support provider has seen a tech clinic summary email, which described these types of capabilities, used as evidence.

Sometimes, the only evidence is evidence that location tracking is occurring, with or without technology. For instance, survivors show messages that indicate the abuser knew where they were. Less commonly, they use cell data to show that the abuser was physically following the survivor.

In summary, survivors use many types of evidence of tech abuse in Wisconsin legal proceedings. As we describe in the next sections, they face several challenges when attempting to prepare (Section 5) and present (Section 6) this evidence.

Table 4. We summarize the seven stages of evidence preparation and presentation and the challenges we identified that are associated with each step.

	Stage	Challenges
Preparing Evidence	Identifying Evidence (§ 5.1)	◊ Surveillance can be intangible, with no evidence to collect. ◊ Evidence might disappear or be deleted before it's needed. ◊ Safety measures like blocking also limit the evidence.
	Prioritizing Evidence (§ 5.2)	◊ Too much evidence can overwhelm the court. ◊ It's hard to know which evidence will be most useful. ◊ What matters to the survivor may not be relevant legally.
	Capturing Evidence (§ 5.3)	◊ Evidence from third parties is hard to get and parse. ◊ Sophisticated collection tools are inaccessible. ◊ Without help, it can be hard to capture evidence legibly. ◊ Time limits hinder evidence capture. ◊ Ongoing abuse hinders evidence capture.
	Preserving Evidence (§ 5.4)	◊ Abusers tamper with and delete evidence. ◊ Giving evidence to others opens authenticity concerns.
Presenting Evidence	Admitting Evidence (§ 6.1)	◊ Required formats vary and are often opaque. ◊ Formatting evidence can be a burden. ◊ Authentication standards for tech are high in practice. ◊ It can be difficult to connect tech abuse to the abuser. ◊ Abusers' attorneys claim missing context or hearsay.
	Making the Case (§ 6.2)	◊ Credibility is key, which harms abuse survivors. ◊ Presenting evidence is a great burden for survivors. ◊ Decisionmakers lack awareness of technology and abuse. ◊ Decisionmakers feel tech abuse belongs in other courts.
	Impacting the Outcome (§ 6.3)	◊ Tech abuse does not always fit legal statutes. ◊ The abuser's intention is hard to prove. ◊ Decisionmakers ignore tech abuse even when it's illegal.

5 Identifying and Capturing Legal Evidence of Tech Abuse

The legal support providers shared insights on how these types of evidence are prepared for and presented in legal proceedings, as well as the challenges to doing so successfully. We present these findings along with the stages that evidence goes through in practice.[5] This section describes how evidence is identified, captured, and stored; then, Section 6 details how evidence is—ideally—admitted, compelling, and impactful to the outcome of the proceedings. In both sections, we emphasize the many challenges survivors face in preparing and presenting legal evidence of tech abuse (Table 4).

5.1 Identifying Evidence to Capture

Once a survivor becomes aware that tech abuse is occurring—assuming they do—their first step is to search for evidence. While sometimes the evidence is apparent, especially for harassment, other times, there is simply no clear evidence to capture.

The legal support providers mentioned that it's often clear their clients are being surveilled, but they don't know how it's happening—with apps, accounts, tracking devices, or just manual stalking. In their experience, it's very hard to prove the existence of surveillance. "*The technology just makes*

[5]The stages may be complex and convoluted, but for the sake of clarity, we present a one-way flow of these stages.

it so much harder because it's so intangible" (P09). P04 noted, "*that more invasive form of abuse of taking over accounts, I've never seen anyone have documentation of that. It's all just verbal accounts.*"

Evidence may disappear before a survivor can preserve it. One way this can happen is if the platform used for tech abuse deletes logs or data after a short period of time. An extreme example is Snapchat, which deletes messages immediately unless they are explicitly saved. Additionally, abusers might delete any trace of the abusive behavior from survivors' devices or social media accounts. For example, in one case of harassment against a young girl, "*it was really hard...to capture anything. He'd post, and then he'd take it down*" (P14). This also came up in cases involving monitoring and surveillance; for example, a client believed their ex had compromised their computer, but upon seeking help, "*they believed that their ex had already erased the traces of their behavior*" (P12).

Complicating this issue is the fact that platform safety measures can sometimes reduce the amount of evidence available. Specifically, survivors often block an abuser's phone number or block them on social media to prevent harassment—but because this measure blocks contact, it also blocks any new evidence coming in that could help the survivor's case:

> *It creates a catch 22, where if you block someone, then they're not contacting you, and then there's no grounds for the restraining order. And if you don't block them, then the judge will be like, "Well, if you were that upset, why didn't you block them?" (P09)*

In addition, a blocked abuser can simply start using proxy phone numbers, which creates additional challenges in proving the abuser is the one doing the harassment (Section 6.1).

5.2 Prioritizing the Evidence

If survivors can find evidence of the tech abuse, they then must decide which pieces of evidence to capture for their proceedings. The legal support providers broadly recommended gathering all possible evidence and including as much supporting information as is available. For a text message, for example, they suggested capturing the date and time a message was sent, ensuring that the abuser's phone number is displayed at the top of the message (as opposed to a contact name), and capturing all texts that came before and after the main text message the survivor wants to capture.

At the same time, it's possible to capture *too much* information that overwhelms survivors, support providers, and legal decisionmakers. "*People send us literally hundreds of pages of texts. And then to print them out, to cut and paste, copy them, and then put them in order and then highlight what are the parts that you want the court to see–that takes hours*" (P12). Advocates, therefore, often help survivors determine what is most useful. "*If you've had experience in court, you can say, 'This is the thing I really want. This is enough to show the context, and I'm going to dump this other stuff because it's just going to overwhelm the court'*" (P19). P14 said, "*Because we do this every day, we know typically what a judge or commissioner is looking for.*" Usually, they are looking for evidence that aligns best with legal statutes.

Even with help from advocates, prioritizing evidence is not always a simple task. Advocates themselves don't always know what will be useful—"*I can suggest call logs, phone records, pictures. … But I think our knowledge and their knowledge of what to look for, what to collect, how to do it, is really limited*" (P02). Further, to emphasize the impact of the abuse, sometimes it is important to show the volume of harassment or give rich context—meaning that reducing the amount of evidence may also reduce this contextual information.

It can also be hard to know how tech abuse fits into the legal statutes, especially with newer forms of tech abuse such as abuse involving smart home devices (Section 6.3). Plus, a survivor's conceptualization of the abuse they faced might not align with the legal statutes. P02 elaborated on this:

> *There's sometimes a disparity with how a certain circumstance makes them feel. They know and identify this is a major part of the abuse, but it doesn't necessarily match the statute, or it doesn't show what they think it's showing from an outside perspective. (P02)*

Thus, what survivors *want* to bring to court to exemplify the abuse they faced is not always the most *relevant* piece of evidence for the proceeding.

5.3 Capturing the Evidence

Next, survivors must capture the evidence they wish to present in court. The most technically sophisticated evidence collection occurs in criminal contexts, where the state has access to resources that are unavailable to laypeople. For example, the state can subpoena technology companies or issue open records requests to get detailed data from devices and accounts. State forensic teams can de-anonymize abusers who hide behind spoofed numbers or false online identities. Police officers can help a survivor investigate, and their implicitly trusted report becomes strong evidence in a trial. This amount of resources can yield extremely useful evidence for survivors: "*There it is, it's all in writing. It's clearer evidence than there's ever been*" (P05).

At the same time, there are challenges to these sophisticated evidence collection methods. Issuing subpoenas to technology companies or cell providers, although tempting, is not always fruitful: "*Generally, Facebook or Instagram or these places are not willing to open up their records really easily*" (P18). There can also be jurisdictional issues, for example, with where the desired data is stored. For one of judge P05's cases involving a camera, "*It's a Chinese company, and they didn't know if they were going to get cooperation or not.*" Finally, evidence can be provided in "*some weird a** format that usually is difficult to understand*" (P07), and sometimes does not contain all necessary information. For example, "*when they extract Tinder messages on Cellebrite,*[6] *it doesn't pick up the emojis*" (P07), which might be key to the message contents.

Moreover, these resources are rarely accessible to *pro se* survivors in civil or family cases. Some survivors attempt to get help from technology companies, forensic experts, or other services to gather more technical evidence, but doing so can be nearly impossible. "*If somebody that has no legal training tried to get records from Snapchat, good luck!*" (P07). Additionally, survivors need some amount of evidence of tech abuse before they can even seek a subpoena—essentially creating a circular dependency, where evidence is required to obtain evidence.

As a result, in civil and family cases, capturing evidence is a mostly unsophisticated process. P09 reflected, "*I don't think I've had any cases where someone did anything Sherlock Holmes-y. It's usually, 'I took a screenshot.'*" For example, survivors capture evidence with screenshots, write logs of their tech abuse experiences, reach out to their cell providers, and search for sources of surveillance (e.g., a GPS tracker). Although uncommon, a couple of legal support providers also mentioned using software that can help compile many texts in an easy-to-read format. Advocates "*try to be as hands on as possible to get to be able to get those things for people in good shape*" (P19).

Although the capturing methods are unsophisticated, survivors still face challenges in capturing the evidence. For example, using screenshots, it's difficult to capture a long text conversation in a way that legibly captures all necessary context. "*You have half of a conversation here, and the whole conversation is repeated down here. And it's really hard to use that as evidence because it's very confusing.*" (P12). For help, some advocates "*refer [the client] to Geek Squad or some expert if it's above my paygrade, which is most technology*" (P07)—but consulting these experts "*might be just really embarrassing and a huge barrier, to go in there and be like, 'Hello, everybody at the counter at the Apple Store. Here's what I'm going through'*" (P12).

[6]Cellebrite [16] is a tool used to collect a suite of data from digital devices.

Importantly, there may be a limited time frame to capture the evidence. In the most extreme case, with restraining orders, there is just a two-week window between filing a restraining order and attending the injunction hearing. P09, who works at a restraining order clinic, said this is a very restrictive timeline:

> *There's no time to try to subpoena the records of which IP sent that email or whatever. … That just doesn't happen in a restraining order. You're not gonna contact Snapchat—even though I know that's a thing, it's never actually deleted. That's just not a resource we have, especially because these are so quick. (P09)*

P14 described a similar concern; their organization has access to a county-wide technical service provider, but survivors often can't use the service due to time constraints:

> *When we need something pretty quick, we can't count on them. Unless it's a huge case with a lot of investigations and the priority gets bumped up. But most of ours wouldn't be considered huge cases. It's one person against one person, and as devastating as that is to those people, in the realm of everything, it wouldn't be deemed an emergency. (P14)*

Less sophisticated methods can also take time, especially given the volume of evidence survivors must go through. One attorney said, "*We ask them to arduously go through sometimes like years of texts with their partner, and send us screenshots. And so you just have to kind of like go by one by one, and then we'll get hundreds of pages*" (P12). There are no shortcuts, either; capturing only a few very salient texts would remove rich contextual details and leave space for an abuser to claim that the conversation was inaccurately represented.

Finally, capturing evidence can be difficult within an abusive situation. For one thing, if an abuser notices that a survivor is saving evidence (e.g., by saving a harassing Snapchat message), the abuser might retaliate, and the abuse could escalate. Another burden is that survivors must avoid responding to the abuse when it happens, or they risk weakening their evidence when it comes time to present it (Section 6.2). For example, if a survivor sends an aggressive response to harassment, an abuser could take that out of context and claim the survivor is the one harassing. To avoid this possibility, attorney P12 tells their clients, "*The court is going to be looking at your texts now. So you have to respond without swearing, without taking the bait, without getting mad.*" Survivors may find it difficult to practice restraint under constant harassment.

Potentially, a survivor may not even conceptualize their experience as abusive while they are in it and therefore doesn't see a need to collect evidence at the time. "*A lot of people just don't expect that they'll need to go that far. [They think,] you'll leave, and the person will forget about you. But it just doesn't happen*" (P09). For some survivors, this means that evidence is long gone by the time they need it. This was the case for one of P04's clients, whose abusive partner was spying on her with in-home cameras: "*She's been out of the home now for, I think, going on a year, and has no way to document that. … She wants the court to be aware of that history, but there's no way for her to present evidence of it aside from her testimony.*"

5.4 Preserving the Evidence

Finally, any evidence that is captured must be stored prior to the legal proceeding. Sometimes, the evidence is just kept by the survivor, ideally somewhere outside their devices in case they are destroyed by the abuser—an unfortunately common occurrence. Carefully preserving evidence is important, given that an abuser may try to tamper with or delete that evidence. Abusers already enacting tech abuse are likely to have access to digital storage systems where survivors keep evidence, and can use that access to delete the evidence. They may also coerce the survivor to delete it: "*I had a couple cases where someone would actually, as part of the control of this person, say 'Give me your phone' and delete things off the phone*" (P08).

Legal support providers recommended that it was best to store evidence in multiple places to avoid losing it. Survivors may thus want to share evidence with a trusted friend, the police, or advocacy groups to help keep it safe. However, any individual entrusted with evidence may need to be involved in the proceeding. P08 said it could happen that "*the opposing party's saying 'That's not what I wrote. And it was in so-and-so's hand? How do I know so-and-so didn't change it?' And so then you would have to bring in [the other] person, and they may not want to be involved.*" Additionally, some organizations have a policy against saving evidence for clients.

Finally, it must be noted that survivors may choose to delete the evidence to protect their well-being. To many survivors, understandably, avoiding that harmful and retraumatizing content is much more important than maintaining evidence for legal proceedings.

With all of these challenges, many survivors are left with only testimony as evidence of the tech abuse they have endured.

6 Presenting Evidence of Tech Abuse in Legal Proceedings

Once evidence is prepared, survivors can attempt to use it in their legal proceedings. We describe three stages of presenting evidence: getting evidence admitted, making a compelling case, and impacting the outcome of the proceedings.

6.1 Getting Evidence Admitted

Evidence cannot be impactful to the proceeding without first being admitted.

6.1.1 Proper formatting. Formatting evidence is the first step to getting evidence admitted. Each court has different rules about how evidence should be formatted; most commonly, the legal support providers reported that courts request evidence in the form of a printed document or as data on a USB stick or a CD. Some courts also allow survivors to e-file evidence by uploading it to, e.g., Axon's Evidence.com [17]. Evidence that is not properly formatted could be rejected by the court, or there may simply be no way to view it, e.g., if "*the client brought their iPhone, and all the courtrooms only have HDMI compatibility*" (P02). At the same time, legal support providers noted that judges occasionally bend these rules—maybe "*officially it's CD, but it depends on the judge*" (P10).

Because different courts (and individual judges) impose different formatting rules, it can be hard to know what to bring. "*Attorneys that aren't regularly presenting evidence in court might not know that, and then certainly somebody who's representing themselves would have no clue*" (P01). This lack of knowledge can directly impact the proceeding, like in one of P02's cases: "*The GAL was like, 'Put these videos on a CD.' They get to the courtroom and the judge is like, 'I don't have a CD player'*" (P02).

To address this opacity, some legal support providers recommended checking with the court to see what format is required; others simply provide every possible format, like P09, who said "*Bring a transcript, bring a USB, bring it on your phone. Print it... Clay tablet...*" Providers wished the rules for accepted formats were more standardized and that those rules were always respected.

Getting evidence in the right format can be tricky, too. For example, "*very few people have the equipment at home to burn a CD*" (P09), and "*a lot of people don't even know how to use the flash drive…It's a lot of extra work that I think the average person would kind of struggle with*" (P01). In other cases, printing evidence can be embarrassing, burdensome, or financially intractable. "*Most clients don't have a printer. They don't want to go to the library or a public place, because 9 times out of 10, what they're printing is pretty embarrassing*" (P14). Legal support providers, therefore, offer to print evidence out, put evidence on digital storage devices, and create copies.

6.1.2 Authenticating evidence. For evidence to be admitted, it must first be authenticated. Survivors typically authenticate evidence using their own testimony, by laying out "*why it's relevant, where it came from, that sort of background*" (P01). To authenticate text messages, for example, they'll answer

questions like "*Is this your cell phone number? Were you texting [abuser's number]? Who did you understand that to be with?*" (P07). If someone else, like a trusted friend, held onto evidence, they may also need to testify to "*the chain of hands that it went through*" (P09). In addition, authentication (especially in criminal cases) can sometimes include testimony from third parties, like an investigator who ran Cellebrite or a representative from a cell phone company.

Legal support providers observed that some judges, aware that technology can be manipulated, assign higher standards to technology-based evidence than they do to other kinds of evidence. Accordingly, it's not uncommon for judges to refuse evidence they cannot confidently authenticate by their standards. A side effect is that if an abuser presents forged counterevidence, a judge might dismiss *both* versions out of caution. P03 described a story like this:

> *[The abuser will] print out whatever the text message looks like that they edited. Our client has the actual text message. But then the judge is like, "Oh, well, I don't know what the actual unedited version is.". … They denied the restraining order because of that, because they're like, "We don't know what the truth is." (P03)*

To combat claims that screenshots or other technology-based evidence have been altered, P17 suggests "*making sure that the survivor doesn't change or edit the photograph in any way.*"

6.1.3 Connecting tech abuse to the abuser. Relevance is also important: the survivor must prove that the abuser was the one performing tech abuse. Unfortunately, abusers tend to hide behind anonymity. P09 described, "*It's so easy to just be like, 'No, I didn't say that. That's not my phone number.'*" Even if survivors have access to the state investigation, they may still be unable to de-anonymize the abuser:

> *They don't put their real names behind it. Or they use like, "cashboy2960" and that's not their real name. But you go and you run that through [forensic service], and it doesn't come back to a name or anything. … A dead end. (P13)*

If abusers use their own accounts or phone numbers for harassment, they still sometimes claim "*'It's not me, I didn't do that, someone hacked my account'*" (P19) or their attorney might say "*Well, we could look at how many people had access to the abuser's phone*" (P06). P19 said, "*I get that a lot*".

The same goes for covert spy devices. Even if a tracking device is found on a survivor's car, it can be hard to prove who placed it there (even if it is painfully clear to the survivor). P18 said identifying *someone* placed a tracker and identifying *who* specifically placed a tracker are very different: "*How do you show who is implanting that technology or watching that technology or perpetrating the abuse through that technology?*"

Sometimes, the problem is proving relevance not to the abuser, but to the *survivor*. For example, P03 described a case where the abuser would harass the survivor on social media, using only her nickname: "*The police said 'Well, he's not naming you, so we can't do anything.' And it's clear to her, and it's clear to all of her friends and family members that he's obviously talking about her*" (P03).

6.1.4 Proving context and completeness. Finally, evidence can be rejected for missing context. "*They can object because there's not a time stamp on it, or it's not clear who's sending these messages*" (P03). Legal support providers see these objections from abusers' attorneys as well as judges. For example, in one case that P06 saw, "*We were printing off like 10 pages of text messages, it's not going to have the date and time on each and every one. … The judge had brought up that they could be out of context.*" Thus, advocates try to "*make sure the client has everything*" (P08).

6.1.5 If evidence is not admitted, it might still be given weight. For example, a GAL can still factor the evidence into their recommendation. However, generally, the evidence would no longer be able to be used in the proceedings. This puts survivors at a disadvantage because decisionmakers "*like*

to have evidence that comes from something other than a person. … Machines, rightly or wrongly, we don't evaluate their credibility or accuracy the same way as we do people" (P07). As we describe in the following subsection, this reliance on credibility is one barrier to making a compelling case.

Additionally, evidence that is not admitted would not be entered into the court record, which can have downstream effects. Specifically, if the decision is appealed—for instance, if the survivor is denied a restraining order, but wants to contest that decision—that evidence could not be used in the appeal, making the appeal less likely to succeed.

6.2 Using Evidence to Make a Compelling Case

Once evidence is admitted, survivors can use it to bolster their case during a legal proceeding. A common theme was that tech-related evidence provides new concreteness to otherwise nebulous forms of abuse, strengthening legal arguments. This may be because, in contrast to forms of evidence like photos of injuries which *corroborate* the abuse, technology is often itself *the tool of abuse.* For example, one of P14's cases:

> *It was just a no brainer. There was no way he or anyone else could fight against it. The proof was there, the date stamp and the timestamp. And it showed that in that 48 hour span, there were 91 calls and texts. And so again, sometimes it [tech abuse] works in our favor to help us.*

This is especially salient for criminal cases, where technology-based evidence is "*usually their strongest evidence. … [It's] the star of the show*" (P07). In civil and family cases, which are more reliant on survivors' testimony, evidence of tech abuse gives important support to the credibility of the testimony.

6.2.1 Reliance on credibility. Along these lines, we learned that no matter what additional evidence the survivor has, "*so much comes down to testimony and credibility*" (P09). P09 described frustration with this paradigm:

> *The judge has to do a credibility assessment. Who's more believable, the person who's saying 'That wasn't me,' or the person who's saying 'I got that call'? … The technology just makes it so much harder because it's so intangible. (P09)*

Decisions come down to credibility even if survivors have concrete evidence beyond their testimony and think, "*We have all this evidence, it's not going to be about credibility*" (P09). One reason is that a judge may not have time to review the evidence, even if it's been admitted. P01 recalled, "*I've heard judges say, 'We only have 30 minutes. If we had all morning, I might look at it.'*" As a result, more and more proceedings rely on testimony and credibility alone.

6.2.2 The burden of presentation. The very real possibility of not being believed makes presenting evidence of tech abuse a great burden for survivors. It is well-documented that abuse survivors, especially those with marginalized identities, face increased scrutiny and bias from judges and other legal stakeholders (see Section 2.3). Our sessions showed that this is also the case for survivors of tech abuse who try to present evidence in Wisconsin legal proceedings.

Due to the importance of credibility, survivors attempt to present themselves as reliable people. "*It's so much pressure to act a certain way*" (P09). However, this is difficult when an abuser is in the same room, arguing against the abuse they have perpetrated; P09 said, "*The client wants to be like, 'That's not true! He's lying!'*" It's also difficult to remain calm when a judge, trying to consider both sides, is skeptical of survivors' claims. "*They're used to everyone telling them they're wrong and that no one believes them. … And then you've got a judge that's now questioning you.*" (P08). P08 described this in more detail:

> *The judge does have to be up there and be very neutral and listen. And I do think that some judges play that line better than others. … Some will show that—maybe because they are very trauma-informed—sometimes they look like they're now favoring the respondent because they're trying to not be so trauma-informed. (P08).*

Finally, these court proceedings can be re-traumatizing experiences for survivors as they must explain the tech abuse they've experienced in detail, in front of the abuser, while facing scrutiny from decision-makers. To illustrate this point, consider a case P09 dealt with, which their client found particularly agonizing:

> *The respondent had all of these photos of our client looking happy on vacation, and he used those photos as evidence to be like "You're smiling and happy. Does this look like somebody who's being abused?". … [The judge] seemed like he was really moved by the photos. He had like a lot of questions. And we were just like, are you kidding? (P09)*

P09 went on to say, "*I feel like you could argue that that was a form of technology abuse.*"

6.2.3 The decisionmaker's interpretation is critical. The specific decisionmaker in a case has an outsize impact on the proceeding, whether it comes down to credibility or not. In particular, the judge in a restraining order proceeding or family court is solely responsible for hearing testimony, admitting and evaluating evidence, and making a final decision. The legal support providers described their frustration with the variability in judges' decisions: even if the evidence is admitted, "*how much weight they give to any particular form of evidence or testimony might change from one of their duty weeks to the next time or from day to day, depending on their mood*" (P04). Although this is true of many types of cases, we see evidence that there may be greater inconsistency when decisionmakers are evaluating evidence of tech abuse.

Many factors can influence how judges and other decisionmakers interpret evidence of tech abuse. Decisionmakers may not understand the technology involved in tech abuse, as P01 described: "*A lot of the judges are not very technology savvy. And so they really will need explanations for everything related to what they're looking at. And I've seen judges get very frustrated, because they don't understand.*" Alternatively, many decisionmakers are unfamiliar with abuse dynamics, especially those who infrequently preside over abuse-related cases. Without the proper background to understand the abuse, decisionmakers might not see how tech abuse is harmful, even if they believe it happened: "*It doesn't matter, right, to the court. It's like, 'Okay, yeah, they said that thing, but I don't really care that they said that thing. It's not that bad'*" (P19). P04 shared another example of this unfortunate phenomenon:

> *Even when a court official might believe one of our clients saying that their ex or abuser was using their accounts or sharing their accounts, and they didn't consent to that, it's minimized sometimes. Or it's discussed as one element of how couples might share things like accounts (P04).*

A lack of knowledge of abuse dynamics can make decisionmakers more likely to believe an abuser's counterarguments. For example, P01 said, "*I've heard of abusers making excuses like, 'Well, I'm just worried about her safety.' Or even like, 'I thought she was cheating on me.' And like judges kind of being like, 'Oh, yeah, it's a messy divorce,' like that is okay.*"

Relatedly, some decisionmakers may interpret that discussions of tech abuse would be best suited for another court context. This can result in a situation where, e.g., a family court judge does not want to discuss tech abuse, but a civil court judge is hesitant to mess with what they see as family court matters—and as a result, the tech abuse does not get addressed. P08 detailed how this happened in a client's case, one that involved harassment:

> *When [family] courts are looking at that, they're like, "They need to learn how to communicate." … So I don't know if taking it to family court is helpful. But I know the civil court, at the same time, is going to be like, "Well, you're two parents and you have to communicate. So if I take away all your ways of communicating, then how are you supposed to co-parent?" (P08)*

Overall, the impact of specific decisionmakers is so great that some attorneys will intentionally avoid specific judges: "*Dismiss and refile in a week. If they're not in major danger right now, I'd wait. I wouldn't even go in front of this judge*" (P08).

6.3 Impacting the Legal Outcome

Once a decisionmaker decides that tech abuse occurred, they must decide whether that tech abuse warrants legal action. Legal support providers emphasized that it is important to precisely describe why the tech abuse they're discussing fits into the legal statutes. "*The statute says this and this, and the respondent's behavior is clearly an example*" (P09). Unfortunately, there are many instances where tech abuse does *not* fit neatly into legal statutes, preventing survivors from getting justice.

6.3.1 Tech abuse does not meet statutes. To begin, there are many times when tech abuse does not meet relevant statutes. For example, P13 (police officer) described, "*if they're just calling, it's not necessarily a crime. So it's not a whole lot that we can do on that ground.*" P01 had similar experiences with social media posts: "*Judges don't consider posting about people, even in cases where they do name them. Like, if they're not tagging them and contacting them in that way, but they're still talking about them on Facebook or Instagram or whatever, it's freedom of speech.*" If tech abuse does not fit the relevant legal statutes by the decisionmaker's interpretation, then it can't be useful in the case.

6.3.2 Statutes have loopholes. In other cases, there are loopholes in the statutes that render tech abuse legal if an abuser claims positive intent. For example, although it is illegal in Wisconsin to track someone using a GPS tracker, it is sometimes legal to use one to track your own child. This can complicate cases where survivors' locations are being tracked by a co-parent:

> *Kids being transferred custody-wise, the parents are taking their stuff, throwing it in the car, and then doing whatever with it.. … The defense was going to be "I had it [the Airtag] in his backpack. … And it must have fallen into the trunk." Of course, the victim was saying, "Absolutely not, she put this in my trunk to track me." (P05)*

The issue of interpreting the intention behind tech abuse spans across multiple forms of tech abuse and, once again, means the proceedings fall back to credibility. P01 says about account compromise: "*Proving that it was intentional and that they didn't consent to it and all of those elements, especially if they're still married, it's a little bit tricky.*" Similar issues of marital property, consent, and ownership can also complicate how tech abuse is adjudicated.

6.3.3 Decisionmakers have final say. However, even if tech abuse *clearly* fits the statutes, decisionmakers sometimes rule in favor of the abuser. For example, P03 has seen this happen with police officers responding to restraining order violations:

> *It's up to the discretion of the police officer responding to the call. So if it's "just one phone call," in quotes, then they might not charge it. [Interviewer: Isn't that still a violation?] Yep. (P03)*

Another time, the judge believed that the survivor had endured constant, horrific harassment from their abuser—but ultimately chose to rule in the abuser's favor because he said he'd change:

> *He [the abuser] said, "Yeah, but I'm an alcoholic, Your Honor. … I'm going to be working on that, I don't think this will be a problem in the future." And the judge said, "Okay.*

> *Yeah, this is really nasty. This is horrible. But going forward, you're gonna have a baby, you're gonna have to learn how to talk with each other." It was bad. (P09)*

Although these examples are disheartening, there is hope—legal support providers also recalled cases where decisionmakers bent statutes or court rules in *favor* of a survivor. For example, "*there are some cases where judges use their discretion to the benefit of survivors of domestic violence to sort of bend the statute. Like, that [type of tech abuse] maybe doesn't technically fit in. . . . [But] that's serving the purpose of the statute*" (P09). Similarly, we heard examples of decisionmakers allowing evidence in forms that are technically not allowed; for example, if a survivor wanted to show a text message on their phone. Perhaps with greater awareness of abuse dynamics and tech abuse, decisionmakers would be more inclined to acknowledge the harms caused by tech abuse and rule in favor of survivors.

7 Discussion

Based on our findings, we offer suggestions for technologists and researchers to support survivors' use of evidence of tech abuse.

Due to the nature of the challenges we identified and similarities across U.S. state legal systems, we envision many of our results would be relevant to other states. For instance, the U.S. legal system broadly hinges on the interpretation of judges and credibility assessments, making it likely that the presentation challenges we identified are felt nationwide. There is also evidence that legal ambiguities and loopholes exist elsewhere—for example, Citron discussed how most U.S. laws for IBSA require proof of malicious intention, and some only apply to publicly-shared images [39].

Nevertheless, many challenges survivors face are agnostic to any specific legal statutes or procedures. For example, there is often no clear evidence to prove that an abuser is conducting tech abuse. Retrieving data from online platforms or manufacturers is burdensome, even with help from the state. Meanwhile, abusers may delete data, escalate abuse, or provide counter-evidence. These challenges relate not to legal frameworks, but to sociotechnical considerations such as technological shortcomings and abuse dynamics. Concerns like these may be relevant to survivors across the U.S. and potentially in other countries, too.

7.1 Call to Action for CSCW Researchers and Technologists

Technologists have an opportunity to support survivors in their evidence collection and presentation pursuits. Here, we draw on our own expertise and the suggestions of the legal support providers to envision future directions.

7.1.1 Platforms should improve the robustness and availability of evidence. The first hurdle for many survivors is a lack of evidence of tech abuse. Thus, we echo calls from prior work [108] that platforms should support survivors by providing more transparency via detailed logs. As the legal support providers noted, evidence of monitoring and surveillance often looks like (1) evidence that *someone* was monitoring the survivor, without pinpointing the abuser, or (2) evidence that the abuser *could have* monitored the survivor, but not that they *used* that ability. Detailed activity logs could help concretize this evidence. For example, apps like FindMy that can be used for location tracking could not only show who has access to a survivor's location, but also each time they check the location. While more detailed logging would certainly be helpful, the logs would need to be easy to find and understand in order to be useful for survivors. We also caution that platform logs are not foolproof evidence, as they can be tampered with or spoofed with relative ease [47].

In addition to providing more evidence, technology needs to better support the preservation of evidence. The legal support providers suggested that messaging apps should store data for longer and show any modifications made, to avoid abusers tampering with or deleting evidence after the

fact. As an example, they pointed to one messaging app, Our Family Wizard [14], that provides these guarantees and is often used by co-parents going through a divorce. Similarly, P13, the police officer, suggested that social media platforms should make public post records easily accessible—and shareable to law enforcement—without a subpoena.

7.1.2 Researchers should develop sociotechnical evidence collection tools. At the same time, we envision sociotechnical evidence collection tools that address survivors' concerns with evidence collection and preservation, while increasing the robustness of the evidence to scrutiny. Existing off-the-shelf tools for evidence collection [13, 15, 36, 111, 116] typically allow survivors to upload photos, screenshots, videos, audio, and text input about an incident. These well-meaning tools do not address many of the challenges we identified (Table 4); for example, they do not support survivors in identifying evidence (Section 5.1), prioritizing the evidence (Section 5.2), or capturing useful and readable information in a short time period (Section 5.3). And several of these apps specifically warn that they might not be admissible in court (Section 6.1). More sophisticated tools motivated by the challenges we identified are sorely needed.

One opportunity to more robustly support evidence collection would be *during* tech clinic interventions (discussed in Section 2). We hypothesize this would be useful because some types of tech abuse we observe regularly in Madison Tech Clinic, such as account compromise, rarely come up in legal proceedings in practice. For instance, P04 noted that they have only ever seen account compromise discussed in testimony, yet there are often clear signs of account compromise, such as a strange login from an unknown location. We believe that a tech-clinic-based intervention could increase the evidence available to survivors without increasing their burden. A key consideration with this type of intervention is that if tech clinic consultants help collect evidence, they could potentially be compelled to testify.

However, not all survivors can access tech clinics. Thus, we envision broader, more accessible resources for a variety of survivors. One such resource could be a software tool, run by survivors on their own, that guides survivors in selecting the evidence they want to collect, prioritizing it, and compiling it in one legible, court-admissible document. A resource like this could reduce survivors' burden, help them feel confident about the content and format required for their case, and even help them identify new evidence. It could also help to standardize evidence of tech abuse, which would increase decisionmakers' familiarity and understanding. However, courts may be less likely to recognize a survivor-led tool, compared to a tool run by expert technology consultants.

Technologists must approach the design of these tools with considerable caution. The most important consideration should be keeping survivors safe. Thus, collaboration with advocates—and, when safe and appropriate, survivors—is crucial. Researchers should also collaborate with legal experts (as was done in, e.g., [53]) to ensure tools are recognized by courts and effective in legal settings. A key piece of this collaboration will be fostering mutual learning [101] through workshops, public resources, and other targeted outreach activities.

7.1.3 Future directions must go beyond sociotechnical tools alone. Finally, we recognize that technology-based interventions to tech abuse are "necessary without being sufficient" [66]. Survivors may not feel comfortable interacting with the legal system [65, 120], or may not want to use technology to address technology abuse [65]. Further, platform changes and sociotechnical evidence collection tools cannot solve the systemic legal problems. Thus, this work must be accompanied by the development of alternative survivor-centered resources, research combating biases in the legal response to abuse survivors (e.g., [78]), and structural changes such as digitization [46] and changes to evidence handling [96, 109] to build a more survivor-centered justice system.

8 Conclusion

We conducted a qualitative study focusing on legal evidence of tech abuse in Wisconsin. Through interviews and focus groups with 19 legal support providers, our study provides insights into the types of evidence survivors use in legal proceedings and the challenges survivors face when attempting to prepare and present evidence of tech abuse in Wisconsin. Specifically, we find 25 challenges survivors must overcome when identifying tech abuse, preparing evidence, and presenting that evidence in court. If evidence of tech abuse exists—which is not always the case—survivors are tasked with capturing, formatting, and prioritizing that evidence in a short time period and often with unsophisticated tools. In the courtroom, a decisionmaker may cast doubt on the authenticity of evidence, minimize the tech abuse proven by the evidence, or argue that the tech abuse is not covered in legal statutes. We argue that addressing these challenges requires a multi-pronged effort, including updates to technology platforms, newly designed sociotechnical evidence collection tools, and structural changes to improve legal options for violence survivors broadly.

Acknowledgments

Many thanks to our participants and the survivors they support, whose experiences are the foundation of this work. The work was greatly improved by help from several groups. Conversations with Ryan Poe-Gavlinski, Jessa Nicholsen, and members of the Restraining Order & Survivor Advocacy Clinic (ROSA) at UW-Madison shaped the research design. PLSC '24 attendees Michele Gilman, Lucy Qin, Jake Chanenson, and Amelia Vance provided valuable feedback. The anonymous reviewers helped us refine this writeup.

We acknowledge funding from the Office for Victims of Crime, Office of Justice Programs, U.S. Department of Justice (Grant # 15POVC-23-GK-01414-NONF). The opinions, findings, and conclusions or recommendations expressed in this paper are those of the contributors and do not necessarily represent the official position or policies of the U.S. Department of Justice.

Finally, we acknowledge the Ho-Chunk Nation on whose ancestral lands we are grateful to work and live as a guest. We deeply respect the knowledge embedded in the Ho-Chunk's custodianship of Teejop (Madison) and recognize their continuing connection to land, water, and community here at the University of Wisconsin–Madison.

References

[1] [n. d.]. Population & Diversity. Data USA: Wisconsin. https://datausa.io/profile/geo/wisconsin?genderResidents=sex2&pums5RacesResident=pums5Race0#demographics Accessed: 2024-2-13.

[2] 2013. Three Basic Methods of Qualitative Text Analysis. In Qualitative Text Analysis: A Guide to Methods, Practice & Using Software, Udo Kuckartz (Ed.). SAGE Publications Ltd, London. http://dx.doi.org/10.4135/9781446288719

[3] 2014. Documentation Tips for Survivors — Safety Net Project. National Network to End Domestic Violence, Safety Net Project. https://www.techsafety.org/documentationtips (Accessed on 10/28/2024).

[4] 2014. SAMHSA's Concept of Trauma and Guidance for a Trauma-Informed Approach. (2014).

[5] 2018. Clinic to End Tech Abuse (CETA). https://www.ceta.tech.cornell.edu/

[6] 2018. Klobuchar Urges Departments of Justice, Health and Human Services to Support Victims of Domestic Abuse in the Digital Age. U.S. Senator Amy Klobuchar. https://www.klobuchar.senate.gov/public/index.cfm/2018/7/klobuchar-urges-departments-of-justice-health-and-human-services-to-support-victims-of-domestic-abuse-in-the-digital-age

[7] 2020. Lorena Gonzalez Announces Legislation to Protect Domestic Violence Survivors from Smart Home Technology Abuses. Assembly Democratic Caucus. https://asmdc.org/press-releases/lorena-gonzalez-announces-legislation-protect-domestic-violence-survivors-smart-home

[8] 2020. Rozic Announces Legislation to Protect Domestic Violence Survivors from Smart Home Technology Abuses. Nily Rozic | Assemply District 25 | Assembly Member Directory | New York State Assembly. https://nyassembly.gov/mem/Nily-Rozic/story/94199

[9] 2021. Devastatingly pervasive: 1 in 3 women globally experience violence. World Health Organization Joint News Release, https://www.who.int/news/item/09-03-2021-devastatingly-pervasive-1-in-3-women-globally-experience-violence.
[10] 2021. Intimate Partner Violence. National Institute of Justice, https://nij.ojp.gov/topics/crimes/violent-crimes/intimate-partner-violence.
[11] 2021. Klobuchar, Murkowski Urge FTC to Protect Domestic Violence Victims' Information Online. U.S. Senator Amy Klobuchar. https://www.klobuchar.senate.gov/public/index.cfm/2021/3/klobuchar-murkowski-urge-ftc-to-protect-domestic-violence-victims-information-online
[12] 2022. Bills Signed: H.R. 7132 and S. 4524. https://www.whitehouse.gov/briefing-room/legislation/2022/12/07/bills-signed-h-r-7132-and-s-4524/. Accessed: 2023-10-3.
[13] 2023. DocuSAFE Documentation and Evidence Collection App. National Network to End Domestic Violence (NNEDV), Safety Net Project. https://www.techsafety.org/docusafe
[14] 2023. OurFamilyWizard - Best Co-Parenting App for Child Custody. OurFamilyWizard.com. https://www.ourfamilywizard.com/ (Accessed on 03/16/2023).
[15] 2023. VictimsVoice – Giving victims a legal voice. VictimsVoice. https://victimsvoice.app/ (Accessed on 03/16/2023).
[16] 2024. Accelerate justice with Cellebrite. Cellebrite. https://cellebrite.com/en/home/ (Accessed on 10/25/2024).
[17] 2024. Axon Evidence. Axon. https://www.axon.com/products/axon-evidence (Accessed on 10/25/2024).
[18] 2024. Court Watch. http://courtwatch.org/.
[19] 2024. Madison Tech Clinic. https://techclinic.cs.wisc.edu/ Accessed: 2024-1-25.
[20] 2024. Victim Advocate Demographics and Statistics: Number Of Victim Advocates In The US. Zippia. https://www.zippia.com/victim-advocate-jobs/demographics/
[21] 2024. Violence Against Women Act. NNEDV. https://nnedv.org/content/violence-against-women-act/ (Accessed on 10/25/2024).
[22] Adrienne E. Adams, Angela K. Littwin, and McKenzie Javorka. 2020. The Frequency, Nature, and Effects of Coerced Debt Among a National Sample of Women Seeking Help for Intimate Partner Violence. Violence Against Women 26, 11 (Sept. 2020), 1324–1342. doi:10.1177/1077801219841445
[23] Majed Almansoori, Andrea Gallardo, Julio Poveda, Adil Ahmed, and Rahul Chatterjee. 2022. A Global Survey of Android Dual-Use Applications used in Intimate Partner Surveillance. Proceedings on Privacy Enhancing Technologies 1 (2022), 20.
[24] Ashwaq Alsoubai, Jihye Song, Afsaneh Razi, Nurun Naher, Munmun De Choudhury, and Pamela J. Wisniewski. 2022. From 'Friends with Benefits' to 'Sextortion:' A Nuanced Investigation of Adolescents' Online Sexual Risk Experiences. Proceedings of the ACM on Human-Computer Interaction (2022), 411:1–411:32. doi:10/gsjrvg
[25] Amna Batool, Mustafa Naseem, and Kentaro Toyama. 2024. Expanding Concepts of Non-Consensual Image-Disclosure Abuse: A Study of NCIDA in Pakistan. In Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems (CHI '24). Association for Computing Machinery, New York, NY, USA, 1–17. doi:10/g8pm89
[26] Rosanna Bellini. 2023. Paying the Price: When Intimate Partners Use Technology for Financial Harm. In Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems. ACM, Hamburg Germany, 1–17. doi:10/gr8rpz
[27] Rosanna Bellini, Kevin Lee, Megan A. Brown, Jeremy Shaffer, Rasika Bhalerao, and Thomas Ristenpart. 2023. The Digital-Safety Risks of Financial Technologies for Survivors of Intimate Partner Violence. In 32nd USENIX Security Symposium (USENIX Security 23). USENIX Association, Anaheim, CA, 87–104. https://www.usenix.org/conference/usenixsecurity23/presentation/bellini
[28] Rosanna Bellini, Emily Tseng, Nora McDonald, Rachel Greenstadt, Damon McCoy, Thomas Ristenpart, and Nicola Dell. 2021. "So-called privacy breeds evil": Narrative Justifications for Intimate Partner Surveillance in Online Forums. Proceedings of the ACM on Human-Computer Interaction 4, CSCW3 (2021), 1–27.
[29] Rosanna Bellini, Emily Tseng, Noel Warford, Alaa Daffalla, Tara Matthews, Sunny Consolvo, Jill Palzkill Woelfer, Patrick Gage Kelley, Michelle L Mazurek, Dana Cuomo, Nicola Dell, and Thomas Ristenpart. 2024. SoK: Safer Digital-Safety Research Involving At-Risk Users. In IEEE Symposium on Security and Privacy (S&P 2024). http://arxiv.org/abs/2309.00735
[30] Arkaprabha Bhattacharya, Kevin Lee, Vineeth Ravi, Jessica Staddon, and Rosanna Bellini. 2024. Shortchanged: Uncovering and Analyzing Intimate Partner Financial Abuse in Consumer Complaints. In Proceedings of the CHI Conference on Human Factors in Computing Systems. 1–20.
[31] Brian Bourke. 2014. Positionality: Reflecting on the research process. The qualitative report 19, 33 (2014), 1–9.
[32] Natalie Grace Brigham, Miranda Wei, Tadayoshi Kohno, and Elissa M. Redmiles. 2024. "Violation of my body:" Perceptions of AI-generated non-consensual (intimate) imagery. In Twentieth Symposium on Usable Privacy and Security (SOUPS 2024). USENIX Association, Philadelphia, PA, 373–392. https://www.usenix.org/conference/soups2024/presentation/brigham

[33] Chay Brown, Mandy Yap, Annick Thomassin, Minda Murray, and Eunice Yu. 2021. "Can I just share my story?" Experiences of technology-facilitated abuse among Aboriginal and Torres Strait Islander women in regional and remote Australia. Journal of Global Indigeneity 5, 2 (2021). https://www.journalofglobalindigeneity.com/article/29716.pdf

[34] Rose Ceccio, Naman Gupta, Majed Almansoori, and Rahul Chatterjee. 2023. Analyzing the Patterns and Behavior of Users When Detecting and Preventing Tech-enabled Stalking. In Proceedings 2023 Symposium on Usable Security. Internet Society, San Diego, CA, USA. doi:10.14722/usec.2023.238140

[35] Rose Ceccio, Sophie Stephenson, Varun Chadha, Danny Yuxing Huang, and Rahul Chatterjee. 2023. Sneaky Spy Devices and Defective Detectors: The Ecosystem of Intimate Partner Surveillance with Covert Devices. In 32nd USENIX Security Symposium (USENIX Security 23). USENIX Association. https://pages.cs.wisc.edu/~chatterjee/papers/usenix23-spydevices.pdf

[36] Women's Center and Shelter of Greater Pittsburgh. 2023. Bright Sky US. App Store. https://apps.apple.com/us/app/bright-sky-us/id1667028531

[37] Rahul Chatterjee, Periwinkle Doerfler, Hadas Orgad, Sam Havron, Jackeline Palmer, Diana Freed, Karen Levy, Nicola Dell, Damon McCoy, and Thomas Ristenpart. 2018. The Spyware Used in Intimate Partner Violence. In 2018 IEEE Symposium on Security and Privacy (SP). ieeexplore.ieee.org, 441–458. doi:10.1109/SP.2018.00061

[38] Jieru Chen, Mikel L Walters, Leah K Gilbert, and Nimesh Patel. 2020. Sexual violence, stalking, and intimate partner violence by sexual orientation, United States. Psychology of violence 10, 1 (2020), 110.

[39] Danielle Keats Citron. 2022. The fight for privacy: Protecting dignity, identity, and love in the digital age. WW Norton & Company.

[40] Dana Cuomo. 2019. Gender-Based Violence and Technology-Enabled Coercive Control in Seattle: Challenges & Opportunities. (2019).

[41] Dana Cuomo. 2022. Coercive Control, Digital Technologies, and Firearms:. (2022).

[42] Dana Cuomo, Nicola Dell, and Alana Ramjit. 2023. The Technology Abuse Clinic Toolkit. (2023).

[43] Dana Cuomo and Natalie Dolci. 2019. Gender-Based Violence and Technology-Enabled Coercive Control in Seattle: Challenges & Opportunities. Technology-Enabled Coercive Control (TECC) Whitepaper Series. https://sites.lafayette.edu/cuomod/files/2021/06/Technology-Enabled-Coercive-Control-Whitepaper-2019-1-1.pdf

[44] Dana Cuomo and Natalie Dolci. 2021. New Tools, Old Abuse: Technology-Enabled Coercive Control (TECC). Geoforum (2021), 224–232. doi:10/gnpfn5

[45] Dana Cuomo and Natalie Dolci. 2022. The TECC Clinic: An innovative resource for mitigating technology-enabled coercive control. Womens. Stud. Int. Forum 92 (May 2022), 102596. https://www.sciencedirect.com/science/article/pii/S0277539522000371

[46] Dana Cuomo and Natalie Dolci. 2023. The Entanglements of the Law, Digital Technologies and Domestic Violence in Seattle. Gender, Place & Culture (2023), 903–923. doi:10/gt57nx

[47] Alaa Daffalla, Marina Bohuk, Nicola Dell, Rosanna Bellini, and Thomas Ristenpart. 2023. Account Security Interfaces: Important, Unintuitive, and Untrustworthy. In 32nd USENIX Security Symposium (USENIX Security 23). 3601–3618. https://www.usenix.org/conference/usenixsecurity23/presentation/daffalla

[48] Jill P Dimond, Casey Fiesler, and Amy S Bruckman. 2011. Domestic violence and information communication technologies. Interact. Comput. 23, 5 (Sept. 2011), 413–421. http://dx.doi.org/10.1016/j.intcom.2011.04.006

[49] Heather Douglas, Bridget A Harris, and Molly Dragiewicz. 2019. Technology-Facilitated Domestic and Family Violence: Women's Experiences. The British Journal of Criminology (2019), 551–570. doi:10/gf64dq

[50] Molly Dragiewicz, Jean Burgess, Ariadna Matamoros-Fernández, Michael Salter, Nicolas P. Suzor, Delanie Woodlock, and Bridget Harris. 2018. Technology Facilitated Coercive Control: Domestic Violence and the Competing Roles of Digital Media Platforms. Feminist Media Studies (2018), 609–625. doi:10/ghqrm8

[51] Molly Dragiewicz, Delanie Woodlock, Michael Salter, and Bridget Harris. 2022. "What's Mum's Password?": Australian Mothers' Perceptions of Children's Involvement in Technology-Facilitated Coercive Control. Journal of Family Violence (2022), 137–149. doi:10/gkgrvc

[52] Kari N. Duerksen and Erica M. Woodin. 2019. Technological Intimate Partner Violence: Exploring Technology-Related Perpetration Factors and Overlap with in-Person Intimate Partner Violence. Computers in Human Behavior (2019), 223–231. doi:10/gr8rpk

[53] Mattia Falduti and Sergio Tessaris. 2022. On the Use of Chatbots to Report Non-consensual Intimate Images Abuses: the Legal Expert Perspective. In Proceedings of the 2022 ACM Conference on Information Technology for Social Good (Limassol, Cyprus) (GoodIT '22). Association for Computing Machinery, New York, NY, USA, 96–102. doi:10.1145/3524458.3547247

[54] Casey Fiesler and Amy S. Bruckman. 2014. Remixers' understandings of fair use online. In Proceedings of the 17th ACM Conference on Computer Supported Cooperative Work & Social Computing (Baltimore, Maryland, USA) (CSCW '14). Association for Computing Machinery, New York, NY, USA, 1023–1032. doi:10.1145/2531602.2531695

[55] Casey Fiesler, Jessica L. Feuston, and Amy S. Bruckman. 2015. Understanding Copyright Law in Online Creative Communities. In Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing (Vancouver, BC, Canada) (CSCW '15). Association for Computing Machinery, New York, NY, USA, 116–129. doi:10.1145/2675133.2675234

[56] Asher Flynn, Anastasia Powell, and Sophie Hindes. 2021. Technology-Facilitated Abuse: A Survey of Support Services Stakeholders. Technical Report. ANROWS Research Report.

[57] Asher Flynn, Anastasia Powell, and Sophie Hindes. 2023. An Intersectional Analysis of Technology-Facilitated Abuse: Prevalence, Experiences and Impacts of Victimization. The British Journal of Criminology (2023), azad044. doi:10/gth3bp

[58] Centers for Disease Control, Prevention, et al. 2018. CDC: 1 in 4 US adults live with a disability. CDC Online Newsroom (2018).

[59] Diana Freed, Sam Havron, Emily Tseng, Andrea Gallardo, Rahul Chatterjee, Thomas Ristenpart, and Nicola Dell. 2019. "Is my phone hacked?" Analyzing Clinical Computer Security Interventions with Survivors of Intimate Partner Violence. Proceedings of the ACM on Human-Computer Interaction 3, CSCW (2019), 1–24.

[60] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. 2018. "A Stalker's Paradise" How Intimate Partner Abusers Exploit Technology. In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems. 1–13.

[61] Diana Freed, Jackeline Palmer, Diana Elizabeth Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. 2017. Digital Technologies and Intimate Partner Violence: A Qualitative Analysis with Multiple Stakeholders. Proc. ACM Hum.-Comput. Interact. 1, CSCW (Dec. 2017), 1–22. https://doi.org/10.1145/3134681

[62] Scott Gleeson. 2022. Woman used an AirTag to track boyfriend, then ran over and killed him, police say. USA Today (June 2022). https://www.usatoday.com/story/news/nation/2022/06/15/woman-airtag-track-boyfriend-death/7632348001/

[63] Michelle M. Graham. 2024. Deepfakes: Federal and state regulation aims to curb a growing threat. Reuters. https://www.thomsonreuters.com/en-us/posts/government/deepfakes-federal-state-regulation/ (Accessed on 10/24/2024).

[64] Naman Gupta, Sanchari Das, Kate Walsh, and Rahul Chatterjee. 2024. A Critical Analysis of the Prevalence of Technology-Facilitated Abuse in US College Students. In Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems (CHI '24). Association for Computing Machinery, New York, NY, USA.

[65] Naman Gupta, Kate Walsh, Sanchari Das, and Rahul Chatterjee. 2024. "I Really Just Leaned on My Community for Support": Barriers, Challenges, and Coping Mechanisms Used by Survivors of Technology-Facilitated Abuse to Seek Social Support. In USENIX Security 2024. Philadelphia, PA.

[66] Diarmaid Harkin and Robert Merkel. 2022. Technology-Based Responses to Technology-Facilitated Domestic and Family Violence: An Overview of the Limits and Possibilities of Tech-Based "Solutions". Violence Against Women (2022), 107780122210883. doi:10/gr8rqb

[67] Bridget Harris and Delanie Woodlock. 2021. Digital Coercive Control and Spatiality: Rural, Regional, and Remote Women's Experience. In The Emerald International Handbook of Technology-Facilitated Violence and Abuse, Jane Bailey, Asher Flynn, and Nicola Henry (Eds.). Emerald Publishing Limited, 387–406. doi:10.1108/978-1-83982-848-520211030

[68] Bridget Harris and Delanie Woodlock. 2022. 'You Can't Actually Escape It': Policing the Use of Technology in Domestic Violence in Rural Australia. International Journal for Crime, Justice and Social Democracy (2022), 135–148. doi:10/gr8rn2

[69] Bridget A Harris and Delanie Woodlock. 2019. Digital Coercive Control: Insights From Two Landmark Domestic Violence Studies. The British Journal of Criminology (2019), 530–550. doi:10/gkxr96

[70] Harris Bridget and Woodlock Delanie. 2022. 'You can't actually escape it': Policing the use of technology in domestic violence in rural Australia. International Journal for Crime, Justice and Social Democracy 11, 1 (March 2022), 135–148. https://doi.org/10.3316/informit.379529323994593

[71] Sam Havron, Diana Freed, Rahul Chatterjee, Damon McCoy, Nicola Dell, and Thomas Ristenpart. 2019. Clinical computer security for victims of intimate partner violence. In 28th USENIX Security Symposium (USENIX Security 19). usenix.org, 105–122. https://www.usenix.org/conference/usenixsecurity19/presentation/havron

[72] Kathryn Haynes. 2012. Reflexivity in qualitative research. Qualitative organizational research: Core methods and current challenges 26 (2012), 72–89.

[73] Alexander Heinrich, Niklas Bittner, and Matthias Hollick. 2022. AirGuard - Protecting Android Users from Stalking Attacks by Apple Find My Devices. In Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks (San Antonio, TX, USA) (WiSec '22). Association for Computing Machinery, New York, NY, USA, 26–38. doi:10.1145/3507657.3528546

[74] Nicola Henry and Asher Flynn. 2019. Image-Based Sexual Abuse: Online Distribution Channels and Illicit Communities of Support. Violence Against Women (2019), 1932–1955. doi:10/gpbtwr

[75] Nicola Henry, Asher Flynn, and Anastasia Powell. 2018. Policing Image-Based Sexual Abuse: Stakeholder Perspectives. Police Practice and Research (2018), 565–581. doi:10/gn7zhh
[76] Nicola Henry and Anastasia Powell. 2018. Technology-Facilitated Sexual Violence: A Literature Review of Empirical Research. Trauma, Violence, & Abuse (2018), 195–208. doi:10/gddz8g
[77] Nicola Henry and Rebecca Umbach. 2024. Sextortion: Prevalence and Correlates in 10 Countries. Computers in Human Behavior (2024), 108298. doi:10/gt6s43
[78] Julie Kaye and Alana Glecia. [n. d.]. Citation for: "Why Do We Have to Be Almost Dead to Qualify for Help?": Criminal Legal and Protection System Responses to Intimate Partner Violence Against Indigenous Women in Canada. Wiley Online Library ([n. d.]).
[79] Roxanne Leitão. 2021. Technology-facilitated intimate partner abuse: a qualitative analysis of data from online domestic abuse forums. Human–Computer Interaction 36, 3 (2021), 203–242.
[80] Isabel Lopez-Neira, Trupti Patel, Simon Parkin, George Danezis, and Leonie Tanczer. 2019. 'Internet of Things': How abuse is getting smarter. Safe – The Domestic Abuse Quarterly 63 (2019), 22–26.
[81] Jeneile Luebke, Peninnah Kako, Alexa Lopez, Marin Schmitt, Anne Dressel, Kathryn Klein, and Lucy Mkandawire-Vahlmu. 2022. Barriers Faced by American Indian Women in Urban Wisconsin in Seeking Help Following an Experience of Intimate Partner Violence. (2022). pmid:36245254 doi:10/gsc3hk
[82] Catherine C. Marshall and Frank M. Shipman. 2015. Exploring the Ownership and Persistent Value of Facebook Content. In Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing (Vancouver, BC, Canada) (CSCW '15). Association for Computing Machinery, New York, NY, USA, 712–723. doi:10.1145/2675133.2675203
[83] Louise Matsakis. 2020. A Hidden Risk for Domestic Violence Victims: Family Phone Plans. Wired (July 2020). https://www.wired.com/story/family-phone-plans-hidden-risk-domestic-violence-victims/
[84] Tara Matthews, Kathleen O'Leary, Anna Turner, Manya Sleeper, Jill Palzkill Woelfer, Martin Shelton, Cori Manthorne, Elizabeth F Churchill, and Sunny Consolvo. 2017. Stories from Survivors: Privacy & Security Practices when Coping with Intimate Partner Abuse. In Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17). Association for Computing Machinery, New York, NY, USA, 2189–2201. https://doi.org/10.1145/3025453.3025875
[85] Jill Messing, Meredith Bagwell-Gray, Megan Lindsay Brown, Andrea Kappas, and Alesha Durfee. 2020. Intersections of Stalking and Technology-Based Abuse: Emerging Definitions, Conceptualization, and Measurement. Journal of Family Violence (2020), 693–704. doi:10/gg6p2g
[86] Teresa E Meuer, Tony Gibart, and Adrienne Roach. 2018. Domestic Abuse: Little Impact on Child Custody and Placement. https://www.wisbar.org/NewsPublications/WisconsinLawyer/Pages/Article.aspx?Volume=91&Issue=11&ArticleID=26737. Accessed: 2023-12-13.
[87] Wendy Moncur, Lorna Gibson, and Daniel Herron. 2016. The Role of Digital Technologies During Relationship Breakdowns. In Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing (San Francisco, California, USA) (CSCW '16). Association for Computing Machinery, New York, NY, USA, 371–382. doi:10.1145/2818048.2819925
[88] World Health Organization et al. 2014. Global status report on violence prevention 2014. World Health Organization.
[89] Simon Parkin, Trupti Patel, Isabel Lopez-Neira, and Leonie Tanczer. 2019. Usability analysis of shared device ecosystem security: Informing support for survivors of IoT-facilitated tech-abuse. In Proceedings of the new security paradigms workshop. 1–15.
[90] Anastasia Powell and Nicola Henry. 2018. Policing Technology-Facilitated Sexual Violence against Adult Victims: Police and Service Sector Perspectives. Policing and Society 28, 3 (March 2018), 291–307. doi:10.1080/10439463.2016.1154964
[91] Anastasia Powell and Nicola Henry. 2019. Technology-Facilitated Sexual Violence Victimization: Results From an Online Survey of Australian Adults. Journal of Interpersonal Violence (2019), 3637–3665. doi:10/gfttwz
[92] Anastasia Powell, Adrian Scott, Asher Flynn, and Nicola Henry. 2020. Image-Based Sexual Abuse: An International Study of Victims and Perpetrators. doi:10.13140/RG.2.2.35166.59209
[93] Hawra Rabaan. 2021. Exploring Transformative Justice Principles to Inform Survivor-Centered Design for Muslim Women in the United States. In Companion Publication of the 2021 Conference on Computer Supported Cooperative Work and Social Computing (Virtual Event, USA) (CSCW '21 Companion). Association for Computing Machinery, New York, NY, USA, 291–294. doi:10.1145/3462204.3481797
[94] Hawra Rabaan and Lynn Dombrowski. 2023. Survivor-Centered Transformative Justice: An Approach to Designing Alongside Domestic Violence Stakeholders in US Muslim Communities. In Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems. 1–19.
[95] Lana Ramjit, Natalie Dolci, Francesca Rossi, Ryan Garcia, Thomas Ristenpart, and Dana Cuomo. 2024. Navigating Traumatic Stress Reactions During Computer Security Interventions. USENIX Security (2024).

[96] Kaitlyn Regehr, Arija Birze, and Cheryl Regehr. 2022. Technology Facilitated Re-Victimization: How Video Evidence of Sexual Violence Contributes to Mediated Cycles of Abuse. Crime, Media, Culture (2022), 597–615. doi:10/gr8rp8

[97] André B Rosay. 2016. Violence against American Indian and Alaska Native Women and Men. NIJ Journal 277 (Sept. 2016). https://scholarworks.alaska.edu/handle/11122/7030

[98] Kevin A Roundy, Paula Barmaimon Mendelberg, Nicola Dell, Damon McCoy, Daniel Nissani, Thomas Ristenpart, and Acar Tamersoy. 2020. The many kinds of creepware used for interpersonal attacks. In 2020 IEEE Symposium on Security and Privacy (SP). IEEE, 626–643.

[99] Nithya Sambasivan, Amna Batool, Nova Ahmed, Tara Matthews, Kurt Thomas, Laura Sanely Gaytán-Lugo, David Nemer, Elie Bursztein, Elizabeth Churchill, and Sunny Consolvo. 2019. "They Don't Leave Us Alone Anywhere We Go": Gender and Digital Abuse in South Asia. In Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19). Association for Computing Machinery, New York, NY, USA, 1–14. doi:10/gr8rpd

[100] Nithya Sambasivan, Garen Checkley, Amna Batool, Nova Ahmed, David Nemer, Laura Sanely Gaytán-Lugo, Tara Matthews, Sunny Consolvo, and Elizabeth Churchill. 2018. "Privacy Is Not for Me, It's for Those Rich Women": Performative Privacy Practices on Mobile Phones by Women in South Asia. In Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018). 127–142.

[101] Devansh Saxena and Shion Guha. 2020. Conducting Participatory Design to Improve Algorithms in Public Services: Lessons and Challenges. In Companion Publication of the 2020 Conference on Computer Supported Cooperative Work and Social Computing (Virtual Event, USA) (CSCW '20 Companion). Association for Computing Machinery, New York, NY, USA, 383–388. doi:10.1145/3406865.3418331

[102] Julia Slupska and Angelika Strohmayer. 2022. Networks of care: Tech abuse advocates' digital security practices. In 31st USENIX Security Symposium (USENIX Security 22). 341–358. https://www.usenix.org/conference/usenixsecurity22/presentation/slupska-networks

[103] Julia Slupska and Leonie Maria Tanczer. 2021. Threat modeling intimate partner violence: Tech abuse as a cybersecurity challenge in the Internet of Things. In The Emerald International Handbook of Technology Facilitated Violence and Abuse. Emerald Publishing Limited.

[104] Sharon G. Smith, Xinjian Zhang, Kathleen C. Basile, Melissa T. Merrick, Jing Wang, Marcie jo Kresnow, and Jieru Chen. 2018. The National Intimate Partner and Sexual Violence Survey (NISVS): 2015 Data Brief – Updated Release. Atlanta, GA: National Center for Injury Prevention and Control, Centers for Disease Control and Prevention, https://www.cdc.gov/violenceprevention/pdf/2015data-brief508.pdf.

[105] Stalking Prevention, Awareness, and Resource Center. 2022. Technology-Facilitated Stalking: Fact Sheet. https://www.stalkingawareness.org/wp-content/uploads/2022/12/SPARC-Stalking-Techology-Fact-Sheet.pdf

[106] Evan Stark. 2007. Coercive control: How men entrap women in personal life. Oxford University Press.

[107] Sophie Stephenson, Majed Almansoori, Pardis Emami-Naeini, and Rahul Chatterjee. 2023. "It's the Equivalent of Feeling Like You're in Jail": Lessons from Firsthand and Secondhand Accounts of IoT-Enabled Intimate Partner Abuse. In 32nd USENIX Security Symposium (USENIX Security 23).

[108] Sophie Stephenson, Majed Almansoori, Pardis Emami-Naeini, Danny Yuxing Huang, and Rahul Chatterjee. 2023. Abuse Vectors: A Framework for Conceptualizing IoT-Enabled Interpersonal Abuse. In 32nd USENIX Security Symposium.

[109] Sophie Stephenson, Lana Ramjit, Thomas Ristenpart, and Nicola Dell. 2025. Digital Technologies and Human Trafficking: Combating Coercive Control and Navigating Digital Autonomy. In Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems (CHI '25). Association for Computing Machinery, New York, NY, USA.

[110] Leonie Maria Tanczer, Isabel López-Neira, and Simon Parkin. 2021. 'I feel like we're really behind the game': perspectives of the United Kingdom's intimate partner violence support sector on the rise of technology-facilitated abuse. Journal of gender-based violence 5, 3 (2021), 431–450.

[111] HeHop Team. 2021. HeHop - Help for Hope. Google Play. https://play.google.com/store/apps/details?id=com.mco.hehop&hl=en&gl=FR (Accessed on 03/16/2023).

[112] Emily Tseng, Rosanna Bellini, Nora McDonald, Matan Danos, Rachel Greenstadt, Damon McCoy, Nicola Dell, and Thomas Ristenpart. 2020. The tools and tactics used in intimate partner surveillance: An analysis of online infidelity forums. In 29th USENIX Security Symposium (USENIX Security 20). 1893–1909.

[113] Emily Tseng, Rosanna Bellini, Alana Ramjit, Thomas Ristenpart, Yeuk-Yu Lee, and Nicola Dell. 2024. Data Stewardship in Clinical Computer Security: Balancing Benefit and Burden in Participatory Systems. In Proceedings of the ACM on Human-Computer Interaction, CSCW. https://emtseng.me/assets/Tseng-2024-CSCW-Data-Stewardship-Digital-Safety_author-version.pdf

[114] Emily Tseng, Diana Freed, Kristen Engel, Thomas Ristenpart, and Nicola Dell. 2021. A Digital Safety Dilemma: Analysis of Computer-Mediated Computer Security Interventions for Intimate Partner Violence During COVID-19. In Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI '21, Article 71). Association for Computing Machinery, New York, NY, USA, 1–17. https://doi.org/10.1145/3411764.3445589

[115] Emily Tseng, Mehrnaz Sabet, Rosanna Bellini, Harkiran Kaur Sodhi, Thomas Ristenpart, and Nicola Dell. 2022. Care Infrastructures for Digital Security in Intimate Partner Violence. In Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems (CHI '22, Article 123). Association for Computing Machinery, New York, NY, USA, 1–20. https://doi.org/10.1145/3491102.3502038

[116] Domestic Violence Resource Centre Victoria. [n. d.]. Arc App. Google Play. https://play.google.com/store/apps/details?id=au.org.dvrcv.arc

[117] Elyse Wild. 2024. New Electronic Evidence Bill Could Help Tribal Courts Bring Justice to MMIP Crisis. Native News Online. https://nativenewsonline.net/health/new-electronic-evidence-bill-could-help-tribal-courts-bring-justice-to-mmip-crisis Accessed: 2024-8-22.

[118] Delanie Woodlock. 2017. The Abuse of Technology in Domestic Violence and Stalking. Violence Against Women (2017), 584–602. doi:10/gg6gv4

[119] Delanie Woodlock and Bridget Harris. 2022. 'You Have to Be Really Careful': Technology and the Abuse of Women with Intellectual and Cognitive Disabilities. Disability & Society (2022), 1–21. doi:10/gscxq6

[120] Delanie Woodlock, Michael Salter, Molly Dragiewicz, and Bridget Harris. 2023. "Living in the Darkness": Technology-Facilitated Coercive Control, Disenfranchised Grief, and Institutional Betrayal. Violence Against Women (2023), 987–1004. doi:10/gscxq7

A Appendix

A.1 Relevant Wisconsin Legal Statutes

Table 5 lists the Wisconsin statutes most relevant to tech abuse. This is not an exhaustive list, nor is it guaranteed that all types of tech abuse will fit into one of these statutes (indeed, we know that some types of tech abuse do not fit any of the statutes).

Received October 2024; revised April 2025; accepted August 2025

Table 5. A summary of the Wisconsin legal statutes most relevant to tech abuse, in order of statute number. With each statute, we list the types of tech abuse (as defined in Table 3) that *might, potentially,* be covered under the statute. These are only approximations; it is a lawyer's job to determine if a specific case matches any of these statutes, some other statute not listed here, or none at all.

Statute	Summary	Tech Abuse
WI §767.405(14)(a)2m: Legal custody and physical placement study†	*Domestic abuse per WI §813.12 (i.e., includes stalking) must be factored into custody and placement decisions.*	🔭📢🖼
WI §813.12: Domestic abuse RO†	*Includes physical or sexual assault,* ***stalking*** *per WI §940.32, or property damage.*	🔭📢🖼
WI §813.125: Harassment RO†	*Includes physical or sexual assault,* ***stalking*** *per WI §940.32, or* ***harassment*** *per WI §947.013.*	🔭📢🖼
WI §940.302: Human trafficking†	*Trafficking someone by means of coercion, threats, intimidation, extortion, deception, or restraint.*	🔭📢🖼
WI §940.315: Global positioning devices†	*Tracking someone's vehicle or movement with a GPS-enabled device without consent.*	🔭
WI §940.32: Stalking†	*Intentionally engaging in a course of conduct—including monitoring/recording, or electronic contact—that would cause a reasonable person distress or fear of bodily injury.*	🔭📢🖼
WI §942.01: Defamation†	*Exposing someone to hatred, contempt, ridicule, degradation or disgrace in society, or injury in their business.*	📢🖼
WI §942.08: Invasion of privacy	*Spying using surveillance devices in a private place with the intent to watch someone nude.*	🔭🖼
WI §942.09: Representations depicting nudity	*Capturing an intimate representation without consent; reproducing, possessing, or distributing an intimate representation that was captured without consent.*	🔭🖼
WI §943.2: Theft	*Taking someone's property (e.g., their phone) without consent and with intent to keep it.*	📢$
WI §943.201: Unauthorized use of an individual's personal identifying information or documents	*Using identifying information—including accounts, or any other information associated with a specific individual—to get something of value, to avoid legal penalties, or to harm the person, their property, or their reputation.*	📢🖼
WI §943.82: Fraud against a financial institution	*Taking money owned by someone else on false pretenses (e.g., using access to their financial accounts).*	$
WI §947.0125: Unlawful use of computerized communication systems	*Using those systems with the intent to frighten, intimidate, threaten, abuse, annoy, or harass someone through electronic messages.*	📢
WI §947.013: Harassment†	*Engaging in a course of conduct or repeatedly committing acts which harass or intimidate another person and which serve no legitimate purpose.*	📢🖼
WI §968.075: Domestic abuse	*Includes physical harm and sexual assault only.*	
WI §968.31: Wiretapping	*One may not intercept and/or disclose electronic communications.*	🔭

† = Statutes explicitly mentioned by the legal support providers.

Types of tech abuse: 📢 = harassment & impersonation, 🔭 = monitoring & surveillance, 🖼 = IBSA, $ = financial abuse.