A Case Study on Legal Evidence of Technology-Facilitated Abuse in Wisconsin

Sophie Stephenson, Naman Gupta, Akhil Polamarasetty[⋆], Kyle Huang, David Youssef,
Rose Ceccio, Kayleigh Cowan[†], Maximilian Zinkus[‡], Rahul Chatterjee
University of Wisconsin—Madison, [⋆]University College London,
[†] Disability Rights Wisconsin, [‡] Johns Hopkins University

Abstract

Abusers use technology to spy on and harass their targets. This pattern is known as *technology-facilitated abuse* (TFA). Survivors of TFA may turn to the legal system to protect themselves, and to do so, they need evidence of TFA. However, prior work indicates challenges to collecting evidence of TFA or using it in legal proceedings. We performed a qualitative case study of legal evidence of TFA in Wisconsin. Through interviews and focus groups with 19 legal professionals, we surface current practices for evidence of TFA in Wisconsin and elucidate several challenges to preparing and presenting evidence of TFA.

1 Introduction

Technology-facilitated abuse (TFA) is a growing problem in the US and globally [7, 8, 10]. Abusive intimate partners, family members, employers, and others have begun to use technology against their targets at alarming rates—in one study, for example, 80% of stalking victims reported being stalked with technology [14]. Unfortunately, different modalities of technology can be misused for stalking or harassment: accounts like Google or email [8], mobile apps designed for spying [6], "dual-use" apps that unintentionally enable spying [6], smart home devices [15, 16], hidden tracking devices [5, 15, 16], and even cars [16]. This type of pervasive abuse can violate a survivor's privacy, isolate them from support systems [10], and sometimes foreshadow physical violence [9].

Survivors of TFA often turn to the legal system to protect their physical and digital safety and security [8]. For example, survivors may file restraining orders [1] to prevent abusers from contacting them under threat of criminal charges, though it is not clear whether these protections prevent abusers from causing harm by remotely exploiting digital devices [3, 12, 15, 16]. Survivors can also argue for favorable restorative custody arrangements in family court proceedings or seek criminal charges against their abusers for illegal acts such as stalking or distribution of non-consensual intimate imagery (NCII). To procure any of these legal protections, survivors need to provide evidence of TFA.

Unfortunately, prior work indicates that survivors face numerous challenges to collecting and presenting evidence of TFA. The onus is on the survivor to "tie the digital abuse to offenses that *are* recognized by the law" [8]—but for some forms of TFA, such as surveillance with smart home devices, it is not clear cut whether those actions are illegal [15]. Similarly, many forms of TFA involve emotional abuse and harassment, which are heavily context-dependent and can be difficult to prosecute. The state-of-the-art of evidence of TFA is hundreds of printed screenshots [8, 11], but it is unclear whether screenshots can capture more elusive forms of TFA, such as account compromise. Finally, support providers and legal professionals have been known to minimize the severity of technology abuse, seeing it as not 'real' compared to physical abuse, or otherwise may lack knowledge of TFA and its harms [8, 15]. These challenges can prevent survivors from getting evidence, not only for legal proceedings but also for "establishing a broader sense of safety and security" [11].

In this work, to better understand the challenges to using evidence of TFA in legal proceedings, we conducted a qualitative case study. We focused on evidence of TFA in legal proceedings in one U.S. state: Wisconsin. Restricting our case study to a single state minimized the complexity of considering varying legal standards between states and focused our analysis on the needs of survivors in this context. Our research questions were:

1. **What is the state of the art for preparing and presenting evidence of TFA in Wisconsin?** For example, what formats of evidence are commonly used, and in what contexts?

USENIX Symposium on Usable Privacy and Security (SOUPS) 2024.
August 11–13, 2024, Philadelphia, PA, United States.

2. **What makes evidence of TFA successful or unsuccessful in Wisconsin legal proceedings?** Are there certain types of evidence to avoid, while others are more likely to be useful in court? Which factors influence this (lack of) success?

2 Method

We used a qualitative instrumental case study [13] to understand evidence of TFA in Wisconsin legal proceedings. We anticipate that though some findings will only relate to specific Wisconsin legal proceedings, other patterns extend to broader contexts.

Interviews & focus groups. We conducted focus groups and interviews with 19 legal professionals to collect their observations and the secondhand experiences of survivors. The participants were over 18 years old who were living and working in Wisconsin and had experience collecting, presenting, or judging evidence of TFA for legal proceedings, or helping survivors with those tasks. We did not interview survivors directly to avoid retraumatization and protect their safety and privacy [4]; as a result, our findings may differ from the experiences of survivors themselves.

We recruited participants through direct emails, phone calls, fliers, and email lists run by a statewide IPV advocacy agency. In total, we conducted 4 focus groups and 8 individual interviews with 19 legal professionals. Participants held roles as legal advocates (e.g., for a domestic violence shelter), attorneys, organization leaders, law clinicians, law enforcement officers, judges, and sexual assault nurse examiners (SANE). Participants work in 9 of the 72 counties of Wisconsin. Participants were offered $20 per hour as compensation.

Procedure. At the start of each session, we asked participants for verbal consent to participate in the study as well as consent to record the session. All participants consented to their session being recorded. We began with warm-up questions asking about the participants' roles and the TFA experiences they have observed. Then, we asked participants about the types of evidence of TFA they have seen in practice, the process for collecting such evidence, and what makes evidence successful or unsuccessful in their experience.

In the last 10 minutes of the interview, we leveraged a design prompt to elicit feedback about an evidence-collection tool we are developing. We described how the tool works, showed participants a mock-up of the evidence document generated by the tool and asked for their thoughts. Using this design prompt not only helped us refine our prototype but also added another dimension to our findings for this study.

Data analysis. We are analyzing the data inductively with Kuckartz's qualitative text analysis methodology [2]. Our process has three stages. In stage one, we generated high-level thematic categories and applied them to our dataset using multiple rounds of collaborative coding (with five coders). Next, we generated subcategories within this codebook and applied them to the data. Now, in the final stage, we are analyzing connections between categories and subcategories.

3 Preliminary Findings

Our preliminary findings show how evidence of TFA is used in practice and the challenges survivors and legal professionals face when using evidence of TFA. These findings will drive changes to court systems, policies, and technology design to better support the use of evidence of TFA. Some preliminary findings are below.

Characterizing evidence of TFA. Participants had observed evidence of TFA in a variety of forms. Photos/screenshots and testimony were by far the most commonly mentioned; other forms of evidence participants had seen included videos (+ transcript), audio (+ transcript), physical devices, cell data, account logs, and summaries of tech clinic consultations. These types of evidence were submitted as printouts or given to the court on digital storage devices (e.g., USB sticks).

Usually, the evidence captured harassment: messages, calls, social media posts, financial abuse, and sharing of non-consensual intimate imagery. Less commonly, the evidence indicated surveillance such as location tracking.

Challenges to capturing evidence. Evidence of surveillance may have been less common because often, there was simply no concrete evidence of the surveillance. Evidence of harassment, too, sometimes disappeared over time, leaving the survivor with nothing.

When evidence did exist, it was difficult to capture that evidence for several reasons. Capturing evidence was time-consuming, especially if there were, e.g., years of harassing texts to document. For more technically-sophisticated evidence collection, survivors could subpoena tech companies or utilize forensic services—but only when they had access to scarce resources like an attorney or police services. Finally, abusers could often access the digital or physical storage places where survivors would preserve evidence.

Challenges to presenting evidence. If evidence could be collected, survivors faced challenges using it in court. Getting evidence admitted was difficult, often because the abuser could not be definitively identified. If evidence was admitted, the greatest challenge was that proceedings greatly relied on the interpretation of decision-makers like judges—people who may not know what TFA is, be familiar with modern technologies, or understand abuse dynamics. Even if survivors could prove TFA, legal definitions sometimes did not cover that abuse or left loopholes that abusers could use to exonerate themselves by, e.g., claiming they were trying to track their child's location, not the survivor's.

Acknowledgements

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 at our session. 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] Wis. stat. § 813.12(1)(am), (1)(b), (1)(c), (5)(d), (2)(c), (3)(c), (2m), (4)(c)(1), (4)(d)(1).

[2] Three basic methods of qualitative text analysis. In Udo Kuckartz, editor, *Qualitative Text Analysis: A Guide to Methods, Practice & Using Software*. SAGE Publications Ltd, London, 2013.

[3] Ahmed Alshehri, Malek Ben Salem, and Lei Ding. Are Smart Home Devices Abandoning IPV Victims? In *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pages 1368–1375, December 2020.

[4] 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. SoK: Safer Digital-Safety research involving At-Risk users. In *IEEE Symposium on Security and Privacy (S&P 2024)*, 2024.

[5] Rose Ceccio, Sophie Stephenson, Varun Chadha, Danny Yuxing Huang, and Rahul Chatterjee. Sneaky spy devices and defective detectors: The ecosystem of intimate partner surveillance with covert devices. In *32nd USENIX Security Symposium (USENIX Security 23)*. pages.cs.wisc.edu, 2023.

[6] Rahul Chatterjee, Periwinkle Doerfler, Hadas Orgad, Sam Havron, Jackeline Palmer, Diana Freed, Karen Levy, Nicola Dell, Damon McCoy, and Thomas Ristenpart. The spyware used in intimate partner violence. In *2018 IEEE Symposium on Security and Privacy (SP)*, page 441–458. ieeexplore.ieee.org, May 2018.

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

[8] Diana Freed, Jackeline Palmer, Diana Elizabeth Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. Digital technologies and intimate partner violence: A qualitative analysis with multiple stakeholders. *Proc. ACM Hum.-Comput. Interact.*, 1(CSCW):1–22, December 2017.

[9] Scott Gleeson. Woman used an AirTag to track boyfriend, then ran over and killed him, police say. *USA Today*, June 2022.

[10] Tara Matthews, Kathleen O'Leary, Anna Turner, Manya Sleeper, Jill Palzkill Woelfer, Martin Shelton, Cori Manthorne, Elizabeth F Churchill, and Sunny Consolvo. Stories from survivors: Privacy & security practices when coping with intimate partner abuse. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, CHI '17, pages 2189–2201, New York, NY, USA, May 2017. Association for Computing Machinery.

[11] Julia Slupska and Angelika Strohmayer. Networks of care: Tech abuse advocates' digital security practices. In *31st USENIX Security Symposium (USENIX Security 22)*, pages 341–358, 2022.

[12] Julia Slupska and Leonie Maria Tanczer. Threat Modeling Intimate Partner Violence: Tech Abuse as a Cybersecurity Challenge in the Internet of Things. In Jane Bailey, Asher Flynn, and Nicola Henry, editors, *The Emerald International Handbook of Technology-Facilitated Violence and Abuse*, Emerald Studies In Digital Crime, Technology and Social Harms, pages 663–688. Emerald Publishing Limited, January 2021.

[13] Robert E. Stake. *Case Studies*, page 435–454. Sage Publications, Inc., 2000.

[14] Stalking Prevention, Awareness, and Resource Center. Technology-Facilitated stalking: Fact sheet, 2022.

[15] Sophie Stephenson, Majed Almansoori, Pardis Emami-Naeini, and Rahul Chatterjee. "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)*, August 2023.

[16] Sophie Stephenson, Majed Almansoori, Pardis Emami-Naeini, Danny Yuxing Huang, and Rahul Chatterjee. Abuse vectors: A framework for conceptualizing IoT-Enabled interpersonal abuse. In *32nd USENIX Security Symposium*, 2023.