

Assessing Evidence of Tech Abuse

Dr. Rahul Chatterjee

Professor,
UW Madison Computer Science

Founder & Director,
Madison Tech Clinic

Sophie Stephenson

PhD Candidate,
UW Madison Computer Science

Director of Operations,
Madison Tech Clinic

Learning Goals

1. Understand how tech abuse occurs in domestic abuse and how safety of victims is impacted.
2. Understand what types of evidence are used to prove tech abuse in Wisconsin legal proceedings.
3. Understand how to assess and authenticate legal evidence of tech abuse.
4. Learn about Madison Tech Clinic and our new evidence-collection initiative.

Notes on Confidentiality

We'll ask for your thoughts and reflections on cases you've seen.

Please do not include:

- Anyone's real name;
- Any information that could identify a specific person.

Intro to Tech Abuse Within Domestic Abuse

Example: Carol



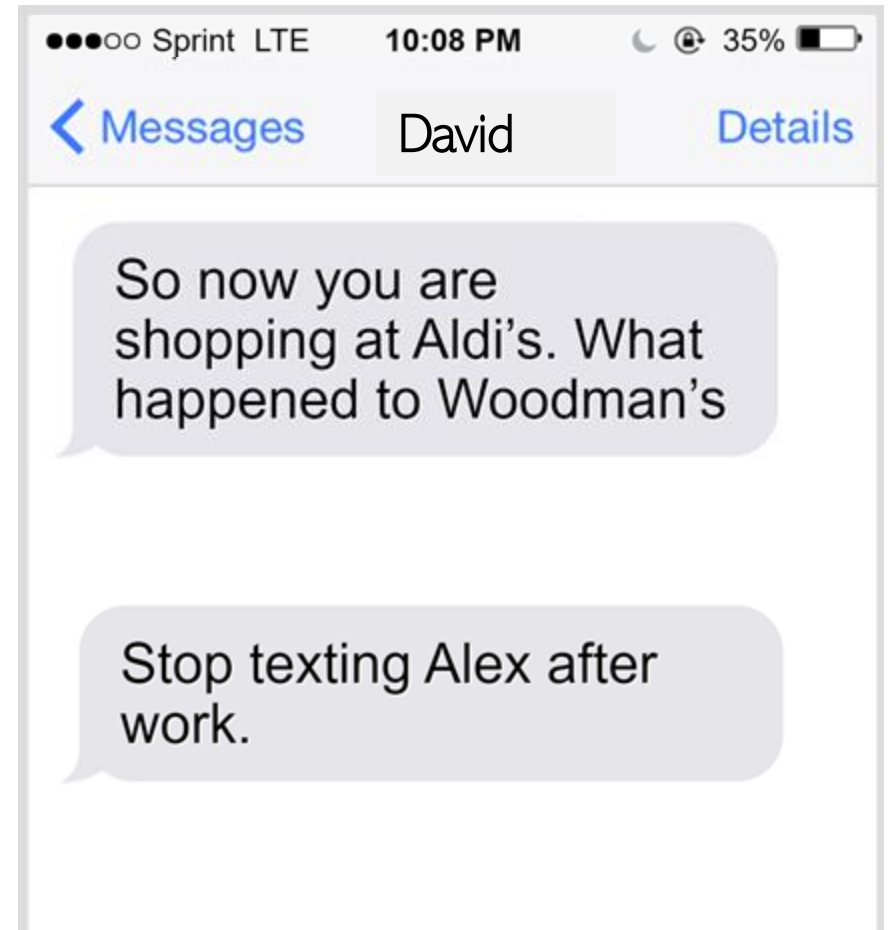
Carol recently separated (divorce pending) from her abusive husband David after years of abuse and control. They have shared custody of a 5-year-old child.

One day her husband sends her a text stating...

A few days later he sends another text...

Carol is confused and terrified:

“How does David know where I go or who I talk to? ... My phone is hacked!”



Technology is a new medium to assert power and control.

Interactivity

Show of Hands:

Who has heard of tech abuse?

(technology-facilitated abuse, digital coercive control, cyberstalking)

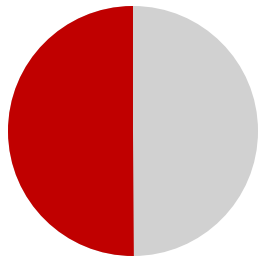
Share Out:

What do you think of when you hear tech abuse?

What is Tech Abuse?

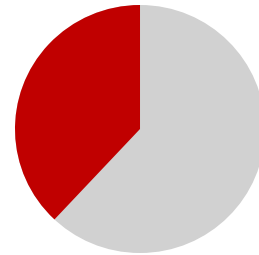
The use of technology to spy on, stalk, harass, and intimidate a target.

intimate partner, family member, victim of human trafficking, stranger...



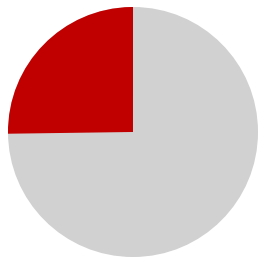
1 in 2

have been targets of online abuse (Thomas 2021)



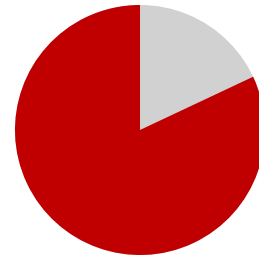
1 in 3

women stalked during their lifetime in the US (CDC 2022)



1 in 4

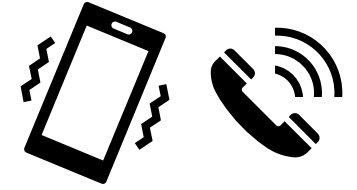
have been targets of **severe** online abuse (Thomas 2021)



4 in 5

stalking victims report being stalked with technology (SPARC 2022)

Types of Tech Abuse: Harassment



Types

Private messages

Phone calls

Public online posts

(Threats to) disclose private info & images

How it Happens

Shared information and social circles

People-search sites

Abuser has intimate images (consensually-shared or not)

Abuser creates AI-generated content

Challenges

Hard to block someone on all platforms

Contact with abuser may be required

Hard to remove content

Blocking & removing content reduces available evidence

Types of Tech Abuse: Account Compromise



Types

Spying on private info

Impersonation

Stealing or deleting digital assets, including money

Account lockout

How it Happens

Accounts already shared between abuser & survivor

Abuser knows/guesses:

- Password
- Authentication factors
- Devices logged in
- Recovery contact info
- Security questions

Challenges

Removing access could lead to abuse escalation

Difficult to tell if an account is compromised

Often no logs of viewing activity (to prove spying)

Financial institutions don't protect against this

Types of Tech Abuse: Spying Apps



Types

Spyware: Apps designed for surveillance

Dual-Use Apps: Apps designed for a benign purpose that can be repurposed for spying.



How it Happens

Physical access to devices (e.g., at time of purchase)

Dual-use apps may have been set up consensually

Children's devices can be used, too

Challenges

Removing apps or sharing could lead to escalated abuse

Identifying spyware is increasingly difficult

Spying apps are available and advertised on and off app stores

Types of Tech Abuse: Smart Devices

Types

Covert spy devices



Smart home devices



Threat to post recordings

How it Happens

Abuser had physical proximity to home or possessions

Abuser lives in the home

Abuser originally set up or had access to smart home devices

Challenges

No good tools to find hidden spy devices

Continued physical presence = they can continue to place more

Smart home devices are often integral to the home

Identifying access is hard

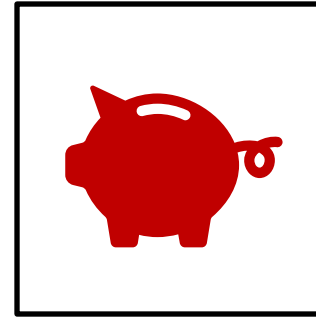
Safety Impacts & Contextual Factors



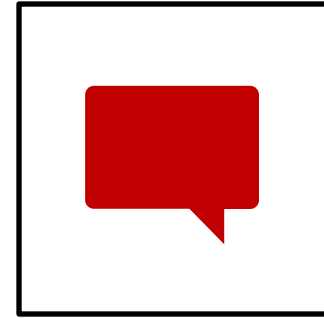
Blocking the
tech abuse
risks retaliation



Living together
prevents many
mitigations



Limited access
to resources



Survivor safety
measures may
resemble tech
abuse

Tech Clinics

Tech Clinics offer one-on-one technical support to survivors.



Photo by KOBU
agency on
Unsplash.

Consultant

Client

Evidence of Tech Abuse

Overview

Tech Abuse and WI Law



Photo by Unknown Author is licensed under [CC BY-SA](#)

Restraining Orders:
Domestic Abuse, Harassment

Family Law:
Custody & placement studies

Criminal Law: Various statutes including stalking, harassment, GPS tracking, invasion of privacy, ...

Notably, NOT domestic abuse.

Interactivity

Share out:

Do you believe tech abuse was involved in any cases over which you've presided?

What types of cases were they?

What evidence was used?

In this section, we'll cover:

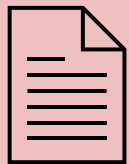
1. A study examining evidence of tech abuse that is used in practice in WI;
2. Broader recommendations on assessing evidence of tech abuse;
3. A pilot program we are running that will provide new forms of evidence of tech abuse.

Evidence of Tech Abuse

Part 1: Our Interview Study

Study Overview

We did interviews and focus groups
with legal support providers
(legal advocates, attorneys, a judge, etc.)



Sophie Stephenson, Naman Gupta, Akhil Polamarasetty, Kyle Huang, David Youssef, Kayleigh Cowan, and Rahul Chatterjee. Legal Evidence of Technology-Facilitated Abuse in Wisconsin: Surfacing Barriers Within and Beyond the Courtroom. ACM CSCW '25.

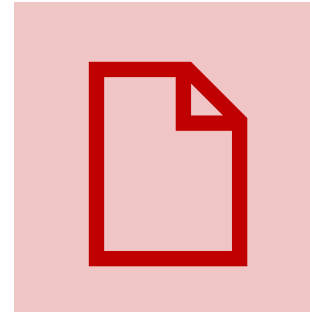
Evidence Types: Capturing Tech Abuse



Screenshots
of harassment,
impersonated
activity, intimate
images...



Recordings
of harassing calls &
voicemails



Records
from cell provider,
tech platforms,
banks...



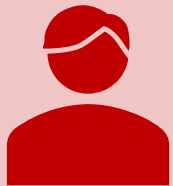
Physical devices
involved in the
tech abuse

Evidence Types: Attributing Abusers



Records

from platforms showing ownership of a phone number, IP address, or online persona

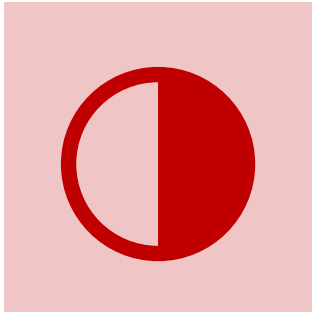


Behavioral attribution

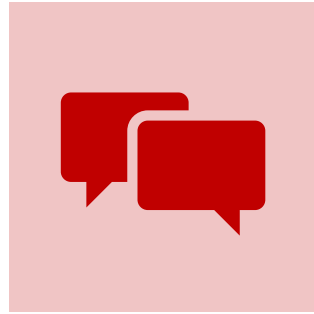
showing similarities between anonymous abuse and the abuser's behavior

E.g., typos & word choice of an anonymous post.

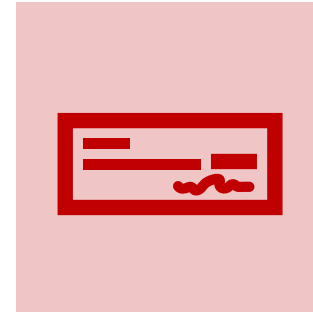
Evidence Types: Circumstantial



Proof of a capability to surveil, but not that that capability was used



Posts or texts talking about perpetrating tech abuse



Records showing purchase of or searching for a spy device online



Indicators of location tracking, without proof that tech was involved

Challenges Preparing Evidence



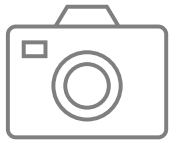
Identifying evidence

Evidence might disappear or not exist in the first place.



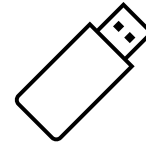
Prioritizing evidence

Difficult to be concise while fitting the burden & giving context.



Capturing evidence

Without state help, means relying on unsophisticated, time-consuming methods.



Preserving evidence

Abusers may tamper or retaliate. Chain of custody issues if given to others.

Challenges Presenting Evidence



Admitting evidence

Roadblocks to authenticating, attributing abuser, and formatting.



Photo by [Tingey Injury Law Firm](#) on [Unsplash](#)



Making the case

Assessment requires understanding tech & abuse. Evidence is contextual & re-traumatizing for survivors.



Impacting the outcome

Tech abuse may not fit vague statutes (+ loopholes). When it does, action is still sometimes declined.

Evidence of Tech Abuse

Part 2: Broader Recommendations

(Un)availability of Evidence

Takeaway 1: Evidence of tech abuse is hard to get.

- Platforms often don't provide sufficient data for evidence.
- Evidence disappears, or is deleted by abuser (or survivor).
- Sophisticated types of evidence are often unreachable.

Recommendation: Expect most evidence to be screenshots, sometimes self-downloaded data, and testimony.

Attributing Tech Abuse

Takeaway 2: Evidence of tech abuse is hard to attribute.

- Deanonymizing usually requires a subpoena.
- Abusers still deny responsibility, even on their own accounts.

Recommendation: Assess anonymous harassment using the content of a message, not just the (lack of) identity of the sender.

Share-out: In cases you've seen, what methods were used to show that the harmdoer was responsible for tech abuse?

Authenticating Tech Abuse

Takeaway 3: Evidence of tech abuse is hard to authenticate.

- Screenshots, and browsers, can be manipulated.
- Data shown on accounts is not always accurate/precise.
- Even metadata can be spoofed (if you're tech-savvy).

This screenshot is fake!

Fake screenshot from "The Trouble with Text Message Screenshots as Evidence," ESI Analyst. <https://esianalyst.com/article/the-trouble-with-text-message-screenshots-as-evidence/>



Authenticating Tech Abuse

Recommendation: What can *you* do to assess authenticity?

- Look for manipulation in fonts, alignment, colors, blurs, timestamps...
- Check metadata: Dates, software & device used, location, format...
- If you can, go to the source! Info viewed on account interfaces, text threads, and social media can typically be deleted but not modified.

Keep an open mind, especially in ROs where there is limited time for collecting, presenting, and (for judges) assessing evidence.

Share-out: How do you go about authenticating digital evidence?
What do you see as the admissibility requirements for digital evidence?

Evidence of Tech Abuse is Varied

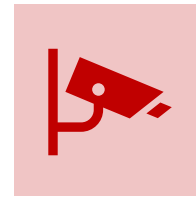
Several potential types that we did not see:



Screenshots showing account compromise



Data takeouts from accounts



Evidence showing smart home abuse

There will be more types as tech evolves, and they won't easily fit current statutory definitions.

Share out: How will you approach new forms of tech abuse as they are brought to your cases?

Evidence of Tech Abuse

Part 3: Our Pilot Program

Our Proposal: Sherlock



Photo by KOBU
agency on
Unsplash.

Consultant

Client



Evidentiary Document

- Spyware apps
- Dual-use apps
- Accounts
- Client comments
- ...

Sherloc Builds on Existing Tools

Builds on **ISDi**:
IPV Spyware Discovery [1],
a locally-run software tool

- Collects list of apps
- Identifies permissions used, install date, etc.
- Highlights suspicious apps



Evidentiary Document

ISDi-collected info

+

Consultant-inputted notes on

- Technology risk assessment
- Account security
- Suspicious app investigations

[1] Havron et al. Clinical Computer Security for Victims of Intimate Partner Violence. USENIX Sec. 2019.

Example Report

Investigation Report

Prepared by the Madison Tech Clinic



Client Name: Sophie Stephenson

Consultation Start Time: 2025/05/15 12:40:06

Information about how the report was generated

This is a summary of a Madison Tech Clinic consultation. The report was generated using a forensic investigative tool developed by Madison Tech Clinic. The tool is available at <https://github.com/madison-tech-clinic/ips-evidence-collector>.

Please see <https://technomic.cs.wisc.edu> or contact techclinic.madison@gmail.com for more information about the Madison Tech Clinic, Sherloc, or this report.

Summary of Findings

Summary page to enable quick understanding

The following are automated summaries generated deterministically.

Technology Assessment Questionnaire

The following risks were identified based on the client's responses to the Technology Assessment Questionnaire:

- ⚠ **Physical access to devices** : A person with physical access to devices might be able to install apps, adjust device configurations, and access or manipulate accounts logged in on that device..
- ⚠ **Shared phone plan** : A shared phone plan may leak a variety of information, possibly including call history, message history (but not message content), contacts, and sometimes location. The account administrator of the client's phone plan has even more privileged access to this information..
- ⚠ **Physical access to children's devices** : A person with physical access to children's devices might be able to install apps, adjust device configurations, and access or manipulate accounts logged in on that device. These changes could allow monitoring of the parent, for example by tracking the children's location when they are with their parent..
- ⚠ **Shared phone plan (child)** : A shared phone plan may leak a variety of information, possibly including call history, message history (but not message content), contacts, and sometimes location. This could include information about the parent, such as their phone number and location when with the children. The plan administrator has even more privileged access to this information..

2 Devices Scanned

Device	Risks Identified
Google Pixel 2, Version 11 (Nickname: Work Pixel)	No risks identified.
Apple iPhone (Model MTM23LL/A), Version 18.5 (Nickname: Personal Phone)	⚠ Risk from app: FindMy : Risks identified: Data leakage..

4 Accounts Checked for Compromise

Account	Risks Identified
Google (Nickname: Personal Google)	⚠ Unrecognized devices : There are unrecognized devices currently logged into this account..

Example Report

Technology Assessment Questionnaire

A set of questions used to assess a client's technology risk factors.

Risk of Device Compromise HUMAN-ENTERED

Question	Response
Do you live with the person of concern?	No
Has the person of concern purchase and/or any of your devices?	No
On which devices did the person of concern purchase and/or set up?	
Has the person of concern had physical access to your devices at any point in time?	Yes
To which devices has the person of concern had physical access?	My personal Macbook
Can the person of concern unlock any of these devices with PIN, password, or biometrics?	No

⚠ Physical access to device
A person with physical access to your devices might be able to install apps, adjust device settings, and access or manipulate accounts logged in on that device.

Annotations to highlight the impact and meaning

Detailed pages with all consultation information

Risk of Account Compromise HUMAN-ENTERED

Question	Response
How do you remember your passwords?	Password manager

⚠ Shared phone plan: A shared phone plan may leak a variety of information, possibly

Pilot Program

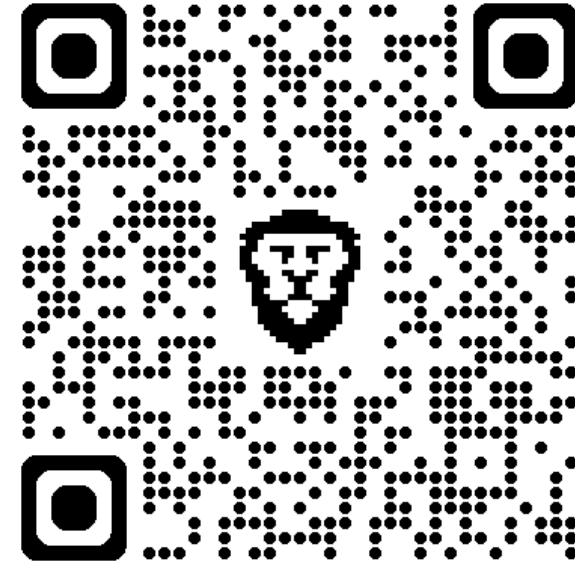
We are currently piloting Sherlock in our in-person consultations.

As it goes on, we're:

- Collecting feedback about it from many stakeholders
- Making changes based on feedback
- Brainstorming new capabilities, e.g., new data sources
- Eventually designing a more advocate- or survivor-led tool

Request for Feedback

If you are willing, please use this QR code or access the URL to fill out a short feedback survey about this document. It should take about 5 minutes.



<https://go.wisc.edu/w11qi3>

Thank you!

Assessing Evidence of Tech Abuse

Dr. Rahul Chatterjee,

Professor at UW Madison | Founder & Director of Madison Tech Clinic

<https://pages.cs.wisc.edu/~chatterjee/> | rahul.chatterjee@wisc.edu

Sophie Stephenson,

PhD Candidate at UW Madison | Director of Operations at Madison Tech Clinic

<https://sophiestephenson.me> | sophie.stephenson@cs.wisc.edu

References

- CDC. The National Intimate Partner and Sexual Violence Survey: 2016/2017 Report on Stalking. 2022.
- Messing et al. Intersections of Stalking and Technology-Based Abuse: Emerging Definitions, Conceptualization, and Measurement. Journal of Family Violence 2020.
- Stalking Prevention, Awareness, and Resource Center (SPARC). Technology-Facilitated Stalking: Fact Sheet. 2022.
- Thomas et al. SoK: Hate, Harassment, and the Changing Landscape of Online Abuse. IEEE S&P 2021.

Additional Questions for Attendees

- What would help us testify most effectively as expert witnesses?
- What could help bolster trust in the document and the way it was created?