Learning Objectives

- Evaluate impact of the misuse of technology on victims.
- Identify common methods of technology misuse that perpetrators of violence employ to control victims.
- Examine the difficult decisions that victims of cyberviolence make when seeking safety and accountability.
- Evaluate admissibility & reliability of technology evidence.

Technology Is Relevant for Judges in Domestic Violence Cases

- Technology can be misused, but can also be an essential tool for victim safety.
- Technology itself is usually neutral.
- In cyberviolence, technology is a piece of the puzzle, but not the entire picture.
Positive Aspects of Technology

- Revolutionized communication
- An essential tool for active participation in many communities
- Important role in the emotional, social, and economic lives of many people

Benefits of Technology

- Many jobs are heavily reliant on technology.
- Artists, activists, and influencers rely on technology.
- For a person with a disability, technology facilitates communication, education, or work.

Technology Use

- The use of technology is common across many groups, however, not all people are similarly situated.
- Survivors of domestic violence may be disproportionately impacted by misuse and loss of access to technology.
Positive Role of Technology for Survivors

- Combating isolation
- Providing opportunity for domestic violence education
- Access to emergency services, mental health services, and advocates
- Access to court systems from rural communities

A Step in Her Digital Footprints

Interactive Exercise

- You will play the role of the main character in the scenario, Soraya.
- We'll then watch a video and make decisions based on evolving facts.
- You will write down your decisions as we go.
Some Decision Points Are Open-Ended

Some Decisions Offer Two Choices, A or B

For Everybody
Background

- Your name is Soraya. You are 27 years old. You live in Houston, Texas. You work as a business analyst for a small marketing firm. However, you have always dreamed of becoming an attorney and you have recently applied to law school.
Background

For the past nine (9) years, you have been in a relationship with your college boyfriend, Solomon. You and Solomon have been living together with your two-year-old son, Alex. With a small child at home, the two of you make enough to get by, but you are living month-to-month.

Background

Solomon works as a software programmer for a small start-up. He makes less money than you do. He works long hours. Solomon was excited when you became pregnant, but as your pregnancy progressed your relationship started to change. You and Solomon began to argue more and more.

Background

After Alex was born, your relationship became increasingly worse. He fluctuated between being impossible to reach when you needed him and constantly checking up on you. When you didn’t answer his calls right away he called your family frantically searching for you.
Background

On one occasion when you were home taking care of the baby, you didn’t answer his call while you were in the shower. He called your neighbor repeatedly and demanded that she go over and check on you and the baby.

Background

Several days ago, you and Solomon got into an intense argument. You tried to leave the house and Solomon stood in front of the door refusing to let you leave. Solomon said, “You will never take my child away from me. After all I have been through, I will fight until the end to make sure I have my family. Nothing will stop me, not even you.”

Background

There was something about the way he said these words that scared you. Later in the evening, the situation calmed down and you were able to leave.
Debrief

- How did it feel making those decisions?
- Were there decisions that were particularly difficult to make?
- Were there points when systems weren’t as helpful as you hoped, or when decisions backfired?

Technology as a Tool of Domestic Violence

- Stalking: Pattern of conduct that causes fear.
- Harassment: Behavior that is aggressive, threatening, frequent, disruptive, etc.
- Impersonation: Representing oneself as someone else.

Technology as a Tool of Domestic Violence

- Surveillance: Tracking location, eavesdropping on conversations, monitoring activities, etc.
- Reputation Harm: Sharing legitimate or false information for the purpose of undermining credibility.
- Fraud and Economic Abuse: Falsely creating or controlling accounts, misusing information, etc.
Learning Points

- Online Violence = Real World Impact.
- Cyberviolence has serious impacts on employment, finances, health, etc.
- Some types of cyberviolence can sound almost unbelievable.
- The intent and impacts of cyberviolence can be just as serious as other types of domestic violence.

Digital Evidence

Digital Evidence Can Be Challenging

- Many judges identify digital evidence as the most important technology concern in their cases.
- Although digital evidence is incredibly important, it can be also confusing, challenging to locate, and at times embarrassing.
Idea Generation

- What are your three biggest challenges with digital evidence?

Digital Evidence Reliability

- Generally, the answer is no.
- All evidence is susceptible to manipulation, especially oral testimony.
- The potential for anonymity with some technology can make proving authorship challenging.

Is Tech Evidence Easier to Manipulate?
Is Tech Evidence Easier to Manipulate?

- There are tools such as photoshop that allow for manipulation, but...
  - Photoshopped images are often recognizable on close inspection.
  - Very good photo manipulation requires a high level of skill.

Is Tech Evidence Easier to Manipulate?

- Tech evidence may have the added benefit of traceability.
- May be able to trace the origin (although it can be difficult, especially for self-represented litigants).
- Changes and modifications are generally identifiable and automatically documented.

Have Rules Caught Up to Technology?

- Tech evidence is just evidence.
- The rules are the same and the issues are (generally) similar.
- While understanding all of the intricacies of technology can be difficult, it is generally not required in order to determine admissibility.
Have Rules Caught Up to Technology?

- Some tech evidence may be harder to evaluate – for example, some tech evidence may require expert testimony.
- However, most tech evidence does not require expert testimony.

Have Rules Caught Up to Technology?

- The majority of tech evidence is admitted like photo evidence, which most courts have done for decades.
- Courts apply the same skills to considering the reliability of tech evidence as with any other type of non-digital evidence.
- In short, you got this!

Weight vs. Admissibility

- The threshold for admissibility is low.
- Evidence is generally admissible if there is reliable information that it is what it purports to be.
- A lack of supporting evidence or incomplete evidence may be a matter of weight, rather than admissibility.
Weight vs. Admissibility

“The possibility of alteration…cannot be the basis for excluding [Electronically Stored Information] as… unauthenticated as a matter of course any more than it can be the rationale for excluding paper documents (and copies of those documents).” US V. Safavian, 644 F. Supp 2d 1 (2009)

Authentication of Digital Evidence

Have Rules Caught Up to Technology?

- What (is digital evidence?)
- Who (can lay a foundation?)
- Where (can evidence be located?)
- When (is the evidence accessible?)
- Why (is the evidence being introduced?)
- How (is the evidence introduced?)
What is digital evidence?

Electronically Stored Information (ESI)
- Information created, manipulated, communicated, stored, and best utilized in digital format, requiring the use of computer or device hardware and software.

What is digital evidence?

Electronically Stored Information (ESI)
- Includes e-mails and attachments, voice mail, instant messaging & other electronic communications, image or video files, word processing docs, text files, hard drives, and metadata (the data about the data).

While Most Digital Evidence is ESI:
- Generally, hard copies of electronically stored documents or evidence presented on digital devices.
- It is important to let litigants (and their attorneys) know in advance if there are limitations or requirements in your courtroom regarding the presentation of evidence.
Electronic Evidence & “Best Evidence”

Rule 1003: Federal Rules of Evidence allows for

- “[a] reproduction created by any process which stores an image of any writing, entry, print, or representation and which does not permit additions, deletions, or changes without leaving a record of such additions, deletions or changes, when authenticated by competent testimony or affidavit which shall include the manner or method by which tampering or degradation of the reproduction is prevented, shall be admissible in evidence as the original.”

Multiple Formats of Digital Evidence

- Collection of numbers and symbols (i.e., IP addresses and metadata).
- Screenshots, pictures, or print outs.
- Screencasts or videos on a different device.
- Written or typed notes
- Copy and pasted reproductions.
- Audio files, images, and graphics.

Who (can lay a foundation?)

- Person who saw the original evidence.
- Person who created or sent the evidence.
- Person who received the evidence.
- Expert who evaluated the evidence or oversaw the device that created, collected, or stored the information.
Where (can evidence be located?)
- Business Records (automatic foundation)
- Litigant devices or 3rd party devices
- Online – including websites, social media, cloud servers, “Wayback Machine,” or internet archives, etc.
- Network records from Internet Service Provider (ISP)
- Storage devices: USB drives, external hard drives, memory cards

When (is the evidence accessible?)
While many devices, networks, and platforms automatically save information, there are large discrepancies in:
- What information is saved.
- How long it is saved.

When (is the evidence accessible?)
Preservation demands may be required to prevent spoliation.
- Many companies automatically delete information in a way that makes it extremely unlikely that the information can be recovered.
Why (is the evidence introduced?)

- Digital evidence can provide especially useful information in domestic violence cases.
- Hearsay is frequently at issue, though numerous exceptions and exemptions may be relevant:
  - Admission by Party Opponent
  - Prior Inconsistent Statement
  - Present Sense Impression

How (can evidence be introduced?)

- Social media postings, text messages, and emails are commonly admitted.
- Print outs are frequently admitted as evidence.
- Circumstantial evidence can be used to connect an account to the accused.

How (can evidence be introduced?)

Examples of circumstantial evidence:

- Username or photos on profile page.
- Personal information on the profile page (i.e., birthday, unique name, or other pedigree).
- Testimony of previous use of number or address.
- Commonly used words, knowledge particular to a person, or actions consistent with message.
Learning Points

- Digital evidence is regularly admitted in digital and non-digital formats.
- The foundation for admissibility is the same with digital evidence as other types of evidence.
- Frequently, the most important consideration is the weight of the evidence, not whether it is admissible.

Learning Points

- Like all evidentiary types, digital evidence may suffer from reliability issues.
- However, digital evidence may have additional reliability safeguards because many digital files have a digital trail that can assist in identifying the origin of the evidence and if the evidence has been modified.
Learning Points

- Digital evidence has a unique ability to assist factfinders in understanding context.
- While digital evidence can provide intimate contextual information, it can also be misleading without a proper context.

Learning Points

- Technology evidence can be difficult to obtain, especially in civil cases.
- The high number of self-represented litigants in domestic violence cases may also increase the challenge of obtaining useful evidence.

Learning Points

- Clearly identifying what evidence is expected, and in what format that evidence should be presented, may lead to more useful evidence.
- Providing access to resources for self-represented litigants about identifying, gathering, collecting, and storing digital evidence can improve the evidence that is ultimately presented in court.
Learning Points

- Circumstantial evidence may be essential for evidentiary foundation and understanding the impact of tech evidence.
- Like most evidence, digital evidence can be "weaponized" by abusive parties to provide a distorted view of events.