1

Support

This project was supported by Grant No. 15JOVW-22-GK-03987-MUMU awarded by the U.S. Department of Justice, Office on Violence Against Women (OVW). The opinions, findings, conclusions, and recommendations expressed in this presentation are those of the authors and do not necessarily reflect the views of the OVW.

2

Fair Use

This presentation includes the creative work of others. This property is being used by permission or under claim of "fair use" (17 USC § 107). This presentation was created pursuant to fair use guidelines and further use or distribution is prohibited.

3

4

Objectives

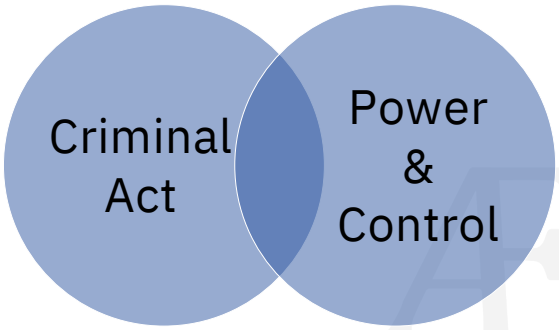
- Make strategic charging decisions that accurately reflect an offender's behavior
- Identify and respond to the use of technology in domestic violence cases with co-occurring stalking.
- Promote thorough investigations and victim safety through collaboration.

5

How have you seen technology misused in cases of intimate partner violence ?

6

Misuse of Technology



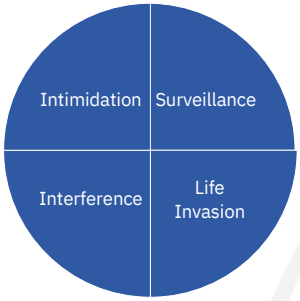
7

The Problem Isn't Technology

- Technology does not cause intimate partner violence; offenders cause intimate partner violence
- Victims should be able to use technology without fear of the offender
- Technology can break isolation and increase victim safety

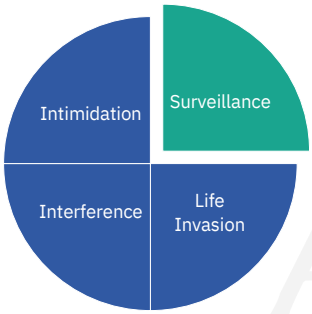
8

SLII Framework



9

SLII Framework
Surveillance



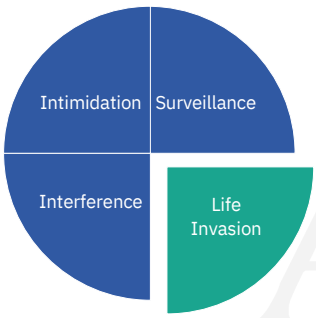
10

Surveillance

- Follow
- Watch
- Wait
- Show up
- Tracking software
- Obtain information about victim
- Proxy stalking

11

SLII Framework
Life Invasion



12

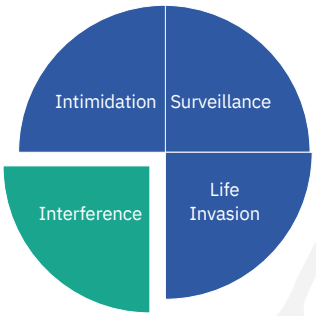
Life Invasion

- Unwanted contact at home, work, etc.
- Showing up
- Phone calls
- Property invasion
- Public humiliation
- Harass friends/family

13

SLII Framework

Interference



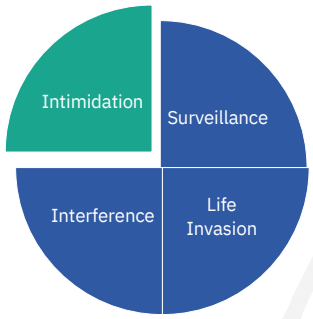
14

Interference

- Financial and work sabotage
- Ruining reputation
- Custody interference
- Keep from leaving
- Road rage
- Attack family/friends/pets
- Physical/sexual attack

15

SLII Framework
Intimidation



16

Intimidation

- Threats
- Property damage
- Symbolic violence
- Forced confrontations
- Threaten or actually harm self
- Threats to victim about harming others

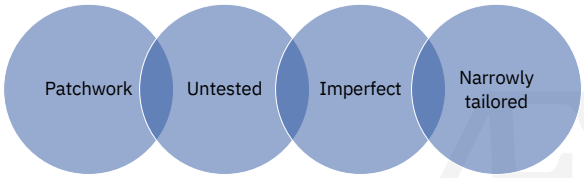
17

Tech-Related Crimes

Harassment	Violation of Protection Order	Video Voyeurism	Invasion of Privacy
Extortion	Wiretapping	GPS Trackers	Nonconsensual Distribution of Intimate Images
Computer Crimes	ID Theft	Witness Intimidation	Obstruction of Justice

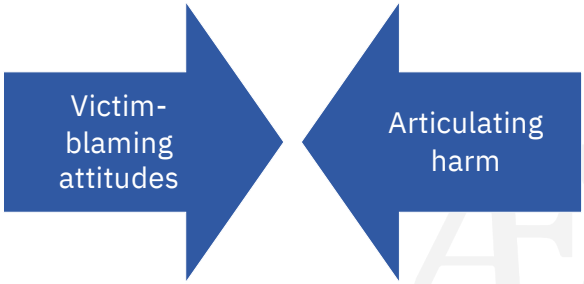
18

Statutory Challenges



25

Additional Challenges



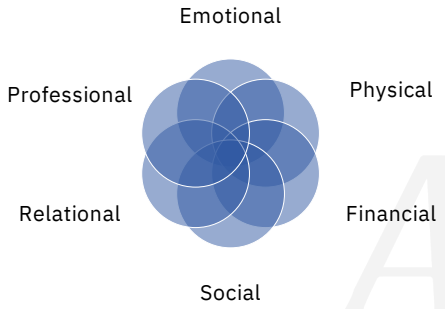
26

Change the Narrative

Victim Blaming	Offender-Focused
• "Boys will be boys" • "Just don't take photos if you don't want them out there" • "Stay off social medial and it wouldn't bother you"	• Offender betrayed a trust • Offender asked for or expected photos as a part of a modern romance • Offender misused technology to prevent the victim from being able to live fully

27

Articulating Harm



28

Identifying and Preserving Digital Evidence

29

Collaborative Approach

30

Benefits

- Tech safety planning
- Educate victim on criminal justice system
- Educate allied professionals about common victim behaviors
- Build trust and rapport
- Provide resources for victim to document stalking and tech-facilitated domestic violence
- Consistent communication
- Support victim through investigation and prosecution

31

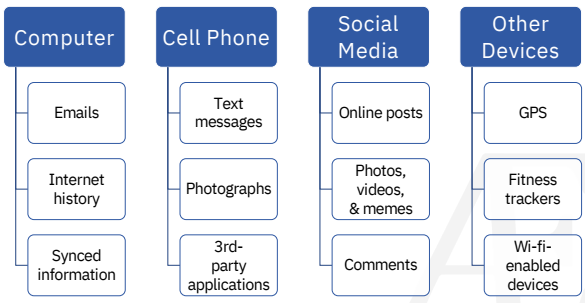
Digital Evidence

Support victims

Build stronger cases

33

Identifying Digital Evidence



34

Related Evidence

Email accounts	App store records	Phone records
Ride share records	Financial records	IP addresses

35

Tools to Seize Digital Evidence

Consent
- Voluntary
- Apparent Authority

Subpoenas
- Subscriber Information
- Transaction History
- IP Addresses

Court Orders
- Location Data
- Tower Dumps
- Wiretap petitions

Search Warrants
- Historical Cell Site Location Information (CSLI)
- Cell Phones
- Social Media
- Computers

This is an area of law that is constantly changing, so please check your local law*

36

Resources

Law enforcement guides and online portals
- Search.org

Listserv
- digital-da+owner@groups.io

New York Prosecutors Training Institute (NYPTI)
- https://www.nypti.org/

King County's Search Warrant Resource Center
- https://warrantportal.kingcounty.gov/justTemplates#warrantsTop

39

Admitting Digital Evidence

40

Purpose of Admission

- Evidence of Crime
- Corroboration
- Context
- 404(b) Evidence

41

Analytical Process

42

What are you admitting?

- Testimony
- Records
- Screenshot / photograph
- Screen recording
- Forensic report
  - HTML document
- Manual examination
  - Video, photos

43

Authenticating or Identifying

Fed. R. Evid. 901

(a) In General. To satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is.

(b) Examples. The following are examples only--not a complete list--of evidence that satisfies the requirement:

44

Authenticating or Identifying

Fed. R. Evid. 901, cont'd.

(1) Testimony of a Witness with Knowledge. Testimony that an item is what it is claimed to be.

...

(4) Distinctive Characteristics and the Like. The appearance, contents, substance, internal patterns, or other distinctive characteristics of the item, taken together with all the circumstances.

...

(8) Evidence About Ancient Documents or Data Compilations....

45

Testimony Alone

U.S. v. Barlow, 568 F.3d 215, 220 (5th Cir. 2009)

- Authentication is not a burdensome standard
- Testimony by a witness with knowledge can be enough to prove authenticity
- The ultimate responsibility for determining whether evidence is what its proponent says it is rests with the jury

46

Establishing Relevance

Linking the Evidence to the Defendant

47

Test for Relevant Evidence

Fed. R. Evid. 401

Evidence is relevant if:

a) it has any tendency to make a fact more or less probable than it would be without the evidence; and

b) the fact is of consequence in determining the action.

48

Making the Link
Circumstantial Evidence

- Where was the device found?
- Who is the account registered to?
  - What is the name on the social media account?
  - Is someone familiar with the regular use of the account?
- Consistent phone records
- Who has access to the photographs?
- Are there words or phrases that are commonly used by the offender?

49

People v. Bonifacio
No. B270882, 2017 WL 4003346, at *3 (Cal. Ct. App. Sept. 12, 2017)

- Instagram photos and accompanying messages were properly admitted via:
  - Screenshots
  - Business records
- Not all screenshots were included in business records, however Court found:

[T]here was "sufficient foundation" for the inference that the posts had been deleted before [the detective] served the subpoena on Instagram and were therefore not included in the Instagram Business Record.

50

Pierce v. State
302 Ga. 389, 396, 807 S.E.2d 425, 433 (2017)

- Screenshots of text messages were properly authenticated and admitted into evidence
- Investigator testified that the images were a "fair and accurate representation" of what appeared on the cell phone screen
- Court also considered that the phone numbers matched as did the content of the communication

51

To the extent the defendant argues that the text messages "could not be authenticated as actually being from [him]," the messages themselves contained sufficient circumstantial evidence tending to show that the defendant was the one who sent them. The sender of the outgoing text messages self-identified himself as "Woo" and "Darius." Multiple witnesses testified that the defendant often went by the nickname, "Woo."

Johnson v. State, 347 Ga. App. 831, 841–42, 821 S.E.2d 76, 86 (2018)

52

State v. Adams

53

Recall from our case file…

On 5/23/23, Anthony Adams posted the following on his public Facebook page:

I just found out my bitch of a wife let our little girl be dragged into a police station and interviewed by the police about a fight she started! If this doesn't stop, I am going to let the whole world know what a crappy mother she is. She neglects our kids and she brought women home for us to have sex with. I have pictures to prove this!

54

Are there any additional crimes you might be able to charge?

How would you use this evidence?

55

New Information

- Anthony is released from jail pending trial and is prohibited from contacting Eva pursuant to a criminal no contact order
- Eva suspects that Anthony has been "spoofing" phone calls and texts
  - Calls and texts look like they are coming from family and friends
  - One text said, "I'm never going to give up on getting through to you. Our kids need both parents."
- Eva also thinks that Anthony has been driving by their house, but Eva has been the only one using the family car

57

How might you work with law enforcement to investigate the spoofing and drive-bys?

Are there other charges you could file?

58

Spoofing

- Subpoena phone records
  - Victim
  - Offender
  - Spoofed number
- Financial records could substantiate the purchase of spoof cards or apps
- App store may have records
- Search of the offender's phone

59

Ride Share Records

- Offenders may use rideshare apps to avoid using a known vehicle
- Subpoena top ride share applications

60

Safeguarding Victim Privacy in a Digital World

Webinar found at:
https://aequitasresource.org/resources/

62

Cell Phones & Privacy

Riley v. California, 134 S. Ct. 2473 (2014)

Court recognized "several interrelated privacy consequences"

- Massive amounts of storage
- Interconnectivity of data
- Information dating back years

...more than 90% of American adults who own cell phones keep on their person a digital record of nearly every aspect of their lives.

63

Motion to Compel

Victim has the phone	Phone is in evidence
• Prosecutor should argue the phone is not in their "care, custody, or control" • Victim is not subject to criminal discovery • Victim Bill of Rights often include the right to privacy and the right to be free of harassment	• Entire phone is not subject to discovery • Defense is going on a fishing expedition • Defense expert has limited access • Protective Order • *In camera* inspection • Redactions

64

"Brady prohibits suppression of evidence, it does not require the government to act as a private investigator and valet for the defendant, gathering evidence and delivering it to opposing counsel."

United States v. Tadros, 310 F.3d 999, 1005 (7th Cir. 2002)

65

National Resources

Safeguarding Victim Privacy in a Digital World, AEquitas Webinar

- https://aequitasresource.org/resources/

Without My Consent, Something Can be Done! Guide

- http://withoutmyconsent.org/resources

Cyber Civil Rights Initiative

- https://www.cybercivilrights.org

National Crime Victim Law Institute

- https://law.lclark.edu/centers/national_crime_victim_law_institute/

66

Going Forward

- Make strategic charging decisions that accurately reflect an offender's behavior.
- Identify and respond to the use of technology in domestic violence cases with co-occurring stalking.
- Promote thorough investigations and victim safety through collaboration.

67