Gathering Technology Abuse Evidence in Protection Order Cases

NCPOFFC webinar
Sept 26, 2018, 12-1:30pm CDT

Ian Harris, JD, MA, Technology Safety Legal Manager, National Network to End Domestic Violence

BATTERED WOMEN'S JUSTICE PROJECT
National Center on Protection Orders and Full Faith & Credit

This project was supported by Grant No. 2016-TA-AX-K052 awarded by the Office on Violence Against Women, U.S. Department of Justice. The opinions, findings, conclusions, and recommendations expressed in this presentation are those of the authors and do not necessarily reflect the views of the Department of Justice, Office on Violence Against Women.

NATIONAL NETWORK TO END DOMESTIC VIOLENCE

Gathering Technology Abuse Evidence in Protection Order Cases

Ian Harris, JD, MA – Technology Safety Legal Manager

This project was supported by Grant No. 2016-TA-AX-K069 awarded by the Office on Violence Against Women, U.S. Department of Justice. The opinions, findings, conclusions, and recommendations expressed in this program are those of the author(s) and do not necessarily reflect the views of the Department of Justice, Office on Violence Against Women.

Safety Net Project

- Addresses **intersection** between technology and abuse.
- Provides **technical assistance and training** to victims, advocates, law enforcement, legal services, social services providers.
- **Advocates** with policymakers and technology companies.

SAFETY NET

What is your profession?

a. Private lawyer
b. Nonprofit lawyer
c. Nonprofit - not an attorney
d. Judge
e. Other?

What do you think is the most difficult tech issue for attorneys?

a. Dynamics of tech abuse

b. Gathering evidence

c. Admitting evidence

d. Getting courts to understand the issues

e. Other?

Helpful Information

- Free speech
- ADA Compliance and Microphones
- Questions…yes please!

Learning Objectives

- Identify common technologies in DV cases
- Understand common tech evidence formats
- Learn how tech evidence is admitted

Why Does Tech Abuse Matter?

Importance to Your Work

- Increased prevalence of technology
- Importance of technology for IPV survivors
- Wealth of evidence available
- This information is often deleted/erased
- It can be difficult to admit this evidence
- Effective dispositions require tech safety
- *Tech evidence can decrease litigation times*

Technology Isn't The Problem – Abuse Is

Technology can:

- enhance and maintain safety
- decrease isolation
- empower survivors

Common Technology

- Mobile devices
- Email & IM
- Global Positioning Systems (GPS)
- Computers
- Social networking sites
- Hidden cameras
- Computer & mobile device spyware
- Assistive technologies
- Smartphone apps

CALLERIDFAKER

Mobistealth

How is Tech Misused in Domestic Violence?

- Stalking
- Surveillance
- Harassment
- Fraud / theft
- Impersonation
- Destroying reputation
- *Tech is a tool, not a type of abuse*

Tech Evidence

Electronically Stored Information (ESI)

- Information created, manipulated, communicated, stored, and best utilized in digital form, requiring the use of computer hardware and software
- Includes e-mails and attachments, voice mail, instant messaging & other electronic communications, word processing docs, text files, hard drives and metadata

Most data used on behalf of DV survivors will be hard copies of electronically stored documents.

Claim of Alteration

- Absent <u>specific</u> evidence showing alteration, courts should not exclude ESI merely because of the <u>possibility</u> of alteration.
- "The possibility of alteration…can not be the basis for excluding [ESI] 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 (1009)

Tip #1: A Little Help Goes a Long Way

- Teach your clients to fish…
    - Teach them how to take screenshots
    - Clearly identify the types of evidence you are seeking
    - Teach them how to identify appropriate evidence and what to do with the evidence
    - Tell them to keep the entire conversation!
- Also, ask them to teach you…

Documenting the Abuse

- Keep a log to establish a pattern of harassment and stalking behavior.
- Take screenshots (computer + phone).
- Take photographs.
- Print out pages.
- Don’t delete emails, text messages, or voicemails.
- Recording options (if legal).

Tip #2: The Early Bird

- Ask *early* about a client’s technology, including any applicable data plans
- Identify evidence that your client can access
- Identify evidence that your adversary can access
- Make a plan to send out evidence requests
- Request evidence from your adversary

How to Improve Evidence

1. Date/Time Stamps
2. Identify connection to the accused
   - Name vs. number
   - Other identifiers
3. Complete
4. Limit manipulation
5. Create a chain of custody
6. Consider legal prohibitions (eavesdropping)

Common Tech Used In Domestic Violence

Direct Communication:

- Texting, Instant Messaging, Email, Spoofing

Social Media:

- Social Networks, Dating Sites, Trolling

***Images:**

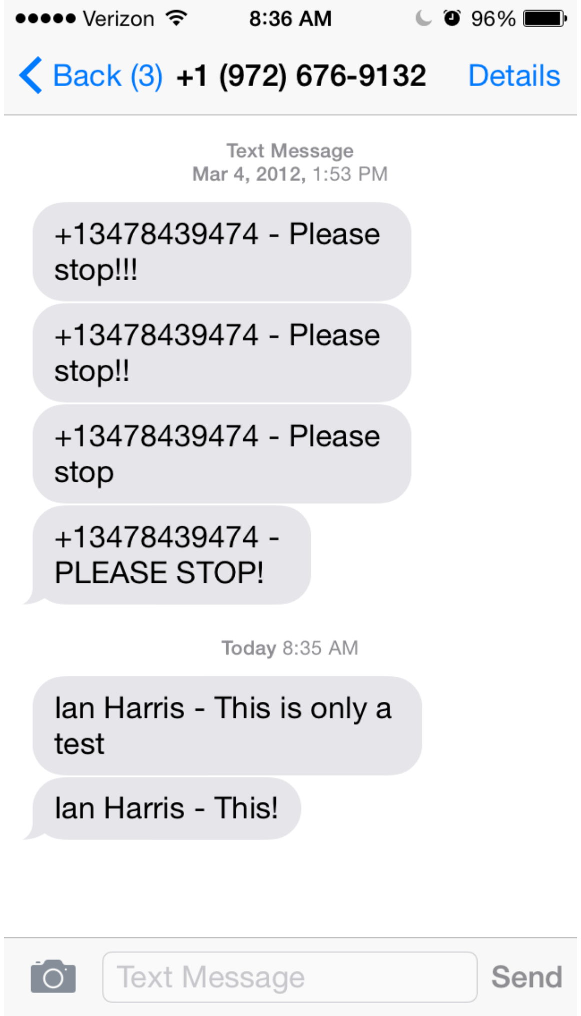
- Photos, Videos, Non-Consensual Sharing

Surveillance & Privacy:

- Spyware, Location Tracking, Online Data

Direct Communication

Text Messages



●●●●● Verizon 8:36 AM 96%

Back (3) +1 (972) 676-9132 Details

Text Message
Mar 4, 2012, 1:53 PM

+13478439474 - Please stop!!!

+13478439474 - Please stop!!

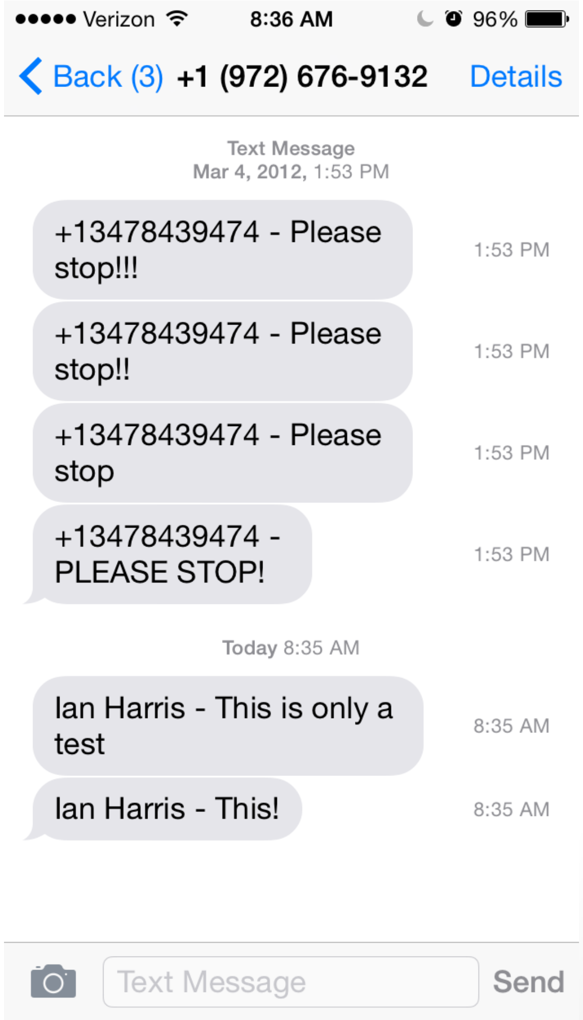
+13478439474 - Please stop

+13478439474 - PLEASE STOP!

Today 8:35 AM

Ian Harris - This is only a test

Ian Harris - This!



●●●●● Verizon 8:36 AM 96%

Back (3) +1 (972) 676-9132 Details

Text Message
Mar 4, 2012, 1:53 PM

+13478439474 - Please stop!!! 1:53 PM

+13478439474 - Please stop!! 1:53 PM

+13478439474 - Please stop 1:53 PM

+13478439474 - PLEASE STOP! 1:53 PM

Today 8:35 AM

Ian Harris - This is only a test 8:35 AM

Ian Harris - This! 8:35 AM

Email – Full Header & IP Address

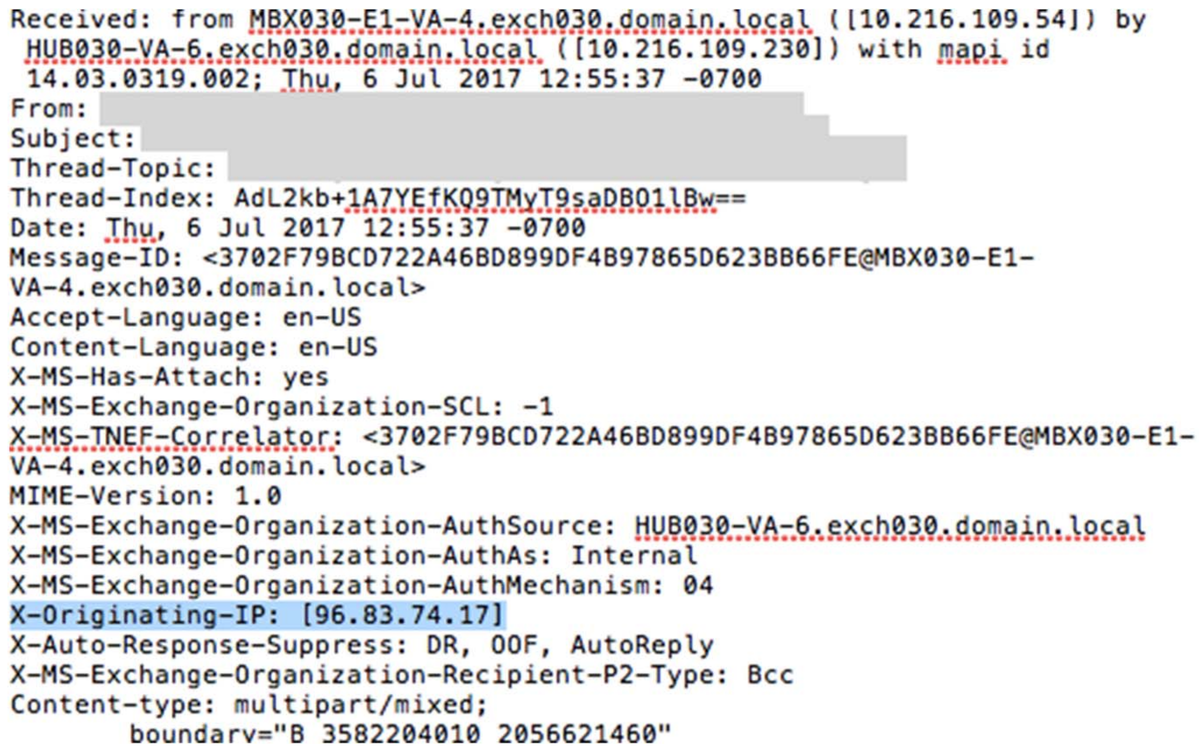
- How do I find the full header?

Google has a tool that outlines how to do this in each of the major webmail providers and email clients http://bit.ly/2tyKaB1

- What do I look for??

Email – Full Header & IP Address

- Look for the **X-Originating IP**



```
Received: from MBX030-E1-VA-4.exch030.domain.local ([10.216.109.54]) by
 HUB030-VA-6.exch030.domain.local ([10.216.109.230]) with mapi id
 14.03.0319.002; Thu, 6 Jul 2017 12:55:37 -0700
From: [redacted]
Subject:
Thread-Topic:
Thread-Index: AdL2kb+1A7YEfKQ9TMyT9saDBO1lBw==
Date: Thu, 6 Jul 2017 12:55:37 -0700
Message-ID: <3702F79BCD722A46BD899DF4B97865D623BB66FE@MBX030-E1-
VA-4.exch030.domain.local>
Accept-Language: en-US
Content-Language: en-US
X-MS-Has-Attach: yes
X-MS-Exchange-Organization-SCL: -1
X-MS-TNEF-Correlator: <3702F79BCD722A46BD899DF4B97865D623BB66FE@MBX030-E1-
VA-4.exch030.domain.local>
MIME-Version: 1.0
X-MS-Exchange-Organization-AuthSource: HUB030-VA-6.exch030.domain.local
X-MS-Exchange-Organization-AuthAs: Internal
X-MS-Exchange-Organization-AuthMechanism: 04
X-Originating-IP: [96.83.74.17]
X-Auto-Response-Suppress: DR, OOF, AutoReply
X-MS-Exchange-Organization-Recipient-P2-Type: Bcc
Content-type: multipart/mixed;
        boundary="B 3582204010 2056621460"
```

Messaging: Authentication

Who can Authenticate?:

- Person who saw the message (recipient, sender, or third party)
  - Testify what the message says (screenshot or the actual phone)
  - Testimony of what a deleted message said
- Phone records (Business Record)

Messaging: Authentication

- **Testimony by "Persons With Knowledge"**
- **"Distinctive Characteristics"** [i.e., Headers] *U.S. v. Safavian, 644 F. Supp. 2d 1 (D.D.C. 2009)*
- **E-Mail Thread – Context** - *U.S. v. Siddiqui, 235 F3d 1318 (11th Cir. 2000)*
- **By Comparison** (previously admitted)
- **By Discovery Production** –the fact that opponent produced emails during discovery can serve as basis for authentication (*John Paul Mitchell Sys. v. Quality Kind Distribs. Inc., 106 F.Supp.2d 462 [SDNY 2000]*)

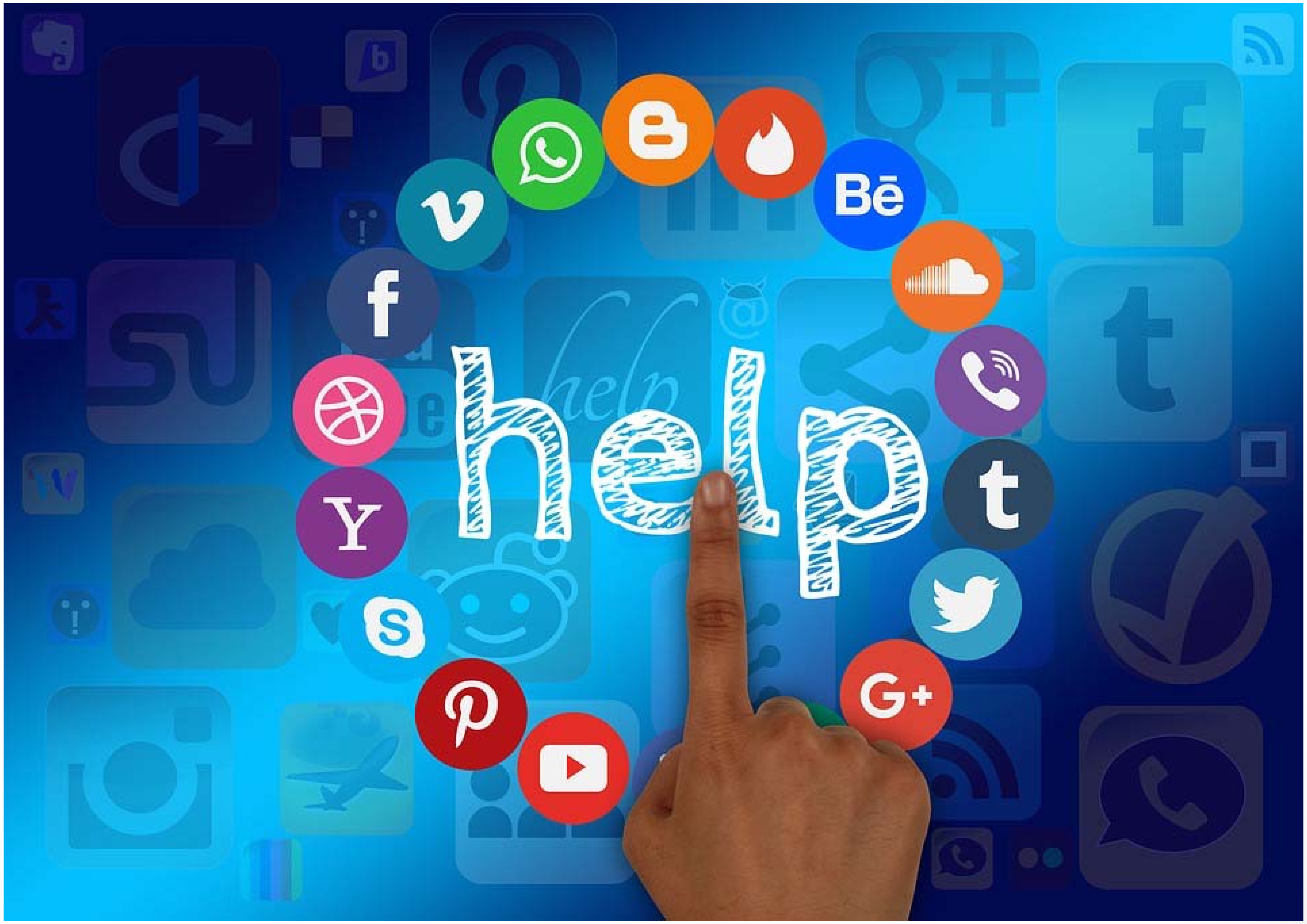
Messaging: Authentication

- **Reply Letter Doctrine** – where recipient replies to an email and refers to the contents of the first email
- **Authentication by Content** (only the author was likely to know the information in the email/text)
- **Authentication by Action Consistent with the Message** – purported recipient takes action consistent with content of message can be circumstantial evidence of authentication

Spoofing

- Spoofing is intentionally deceiving another by sending false identifying information
  - *Email*
  - *Phones*
  - *Any device that receives sender information*
- Lawful and unlawful purposes
- Usually requires fraud to be illegal
- Can be difficult to prove

Social Media



Social Media Misuse

- Changing passwords
- Access to accounts w/o consent
    - Deleting information
    - Sending fraudulent messages
    - Posting rumors
    - Intercepting messages
- Creating false virtual profiles on dating or pornographic sites
    - Posting sexual or pornographic images or text

Additional Negative Impact

- Community impact
  - Outsourcing abuse (bullying)
  - Social abuse
  - Particularly dangerous for marginalized groups
- Impact on career and/or school
- Cost in time and money

Social Networking Evidence

- **Testimony: screenshot was actually on the website**
- **It accurately depicts what was on the website**
- **The content is attributable to the owner***

[Lorraine v. Markel Amer. Ins. Co., 241 F.R.D. 534 (D. Md. 2007)]

*Some courts require website owner to authenticate.

Social Networking Evidence

- **The owner testifies to posting it**
- **Forensic computer expert testifies** that she examined the hard drive and was able to recover the posting

OR

- **Circumstantial Evidence Permissible**:

  -Printout has the username shown on profile page

  -Is there a photo on the persons profile page that identifies a person as the poster

  -Is there personal information on the profile page (i.e., birthday, unique name, other pedigree)

Images

Misuse of Images

- Voyeurism
- Child pornography (grooming)
- Pictures/videos taken of consensual sex, distributed without consent
- Up-skirting and down-blousing
- Surveillance/spying
- Pictures/videos taken of physical and sexual assaults

Non-Consensual Intimate Images (NCII)

- Sexually explicit images or video **taken** and/or **shared** without consent of person.
- Content is obtained:
  - Voluntarily, shared within trusted relationship.
  - Hidden cams, up-skirting, down-blousing.
  - Stolen photos, hacking into computers.
  - Blackmail & tricking victims.
- Personal information also often shared.

Beware the "Deep Fake"

Surveillance & Privacy

Monitoring & Info Gathering

- Physically examining devices
- Examining phone records (online or paper)
- Checking voicemail
- Logging onto online account to change or activate settings and features
- Tracking location via phone, app.
  - Family location features, find my phone

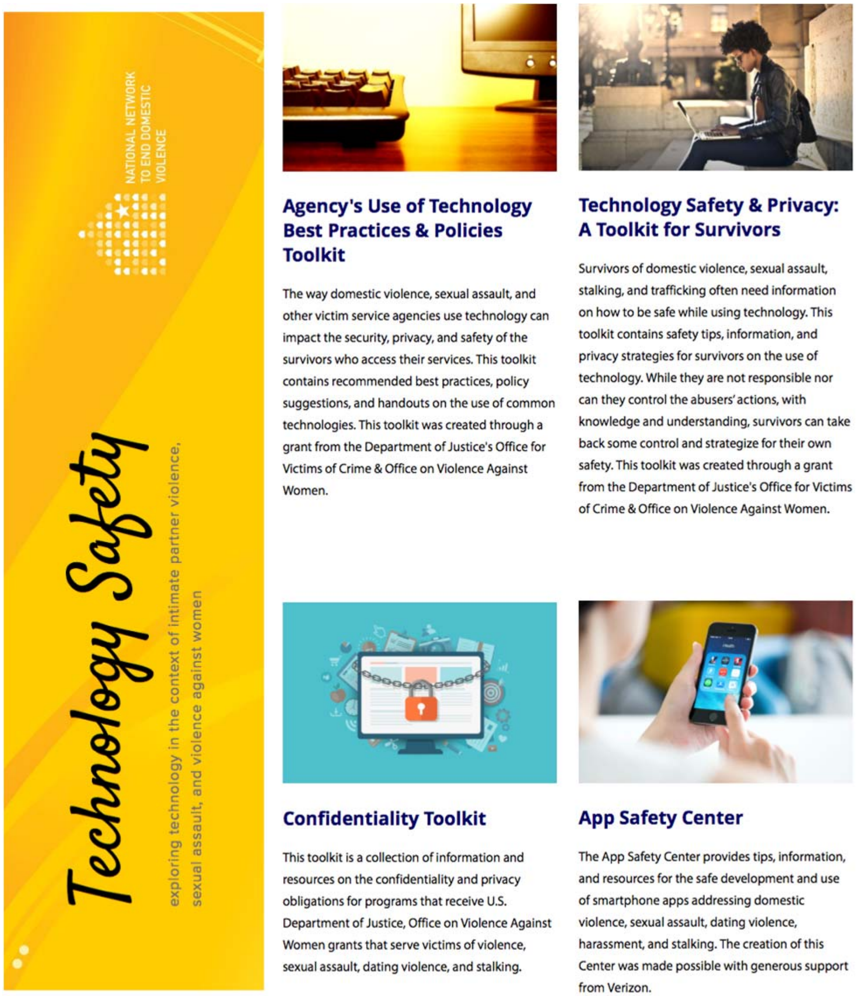
Detecting Spyware

- Unusual battery drain or battery warm when not in use
- Spikes in data usage
- May take longer to shut down
- Screen may light up when not using
- May hear clicks or sounds when on calls
- Additional incoming calls on bill that user didn't receive
- Abuser knows things that s/he could only know if they have access to the phone
- Perpetrator has or had physical access

QUESTIONS?

RESOURCES

TechSafety.org/resources



NATIONAL NETWORK TO END DOMESTIC VIOLENCE

Technology Safety

exploring technology in the context of intimate partner violence, sexual assault, and violence against women

Agency's Use of Technology Best Practices & Policies Toolkit

The way domestic violence, sexual assault, and other victim service agencies use technology can impact the security, privacy, and safety of the survivors who access their services. This toolkit contains recommended best practices, policy suggestions, and handouts on the use of common technologies. This toolkit was created through a grant from the Department of Justice's Office for Victims of Crime & Office on Violence Against Women.

Technology Safety & Privacy: A Toolkit for Survivors

Survivors of domestic violence, sexual assault, stalking, and trafficking often need information on how to be safe while using technology. This toolkit contains safety tips, information, and privacy strategies for survivors on the use of technology. While they are not responsible nor can they control the abusers' actions, with knowledge and understanding, survivors can take back some control and strategize for their own safety. This toolkit was created through a grant from the Department of Justice's Office for Victims of Crime & Office on Violence Against Women.

Confidentiality Toolkit

This toolkit is a collection of information and resources on the confidentiality and privacy obligations for programs that receive U.S. Department of Justice, Office on Violence Against Women grants that serve victims of violence, sexual assault, dating violence, and stalking.

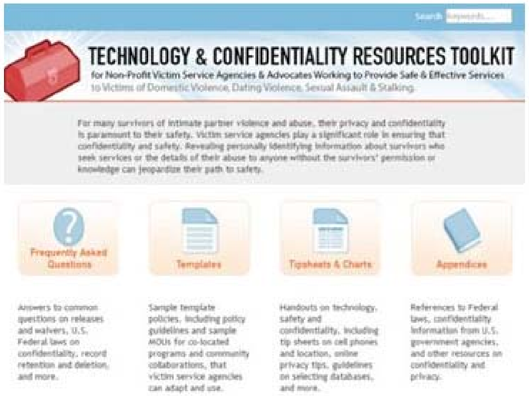
App Safety Center

The App Safety Center provides tips, information, and resources for the safe development and use of smartphone apps addressing domestic violence, sexual assault, dating violence, harassment, and stalking. The creation of this Center was made possible with generous support from Verizon.

Resources & Toolkits

Agency's Use of Technology Best Practices & Policies Toolkit

Technology Safety & Privacy: A Toolkit for Survivors



TECHNOLOGY & CONFIDENTIALITY RESOURCES TOOLKIT

for Non-Profit Victim Service Agencies & Advocates Working to Provide Safe & Effective Services to Victims of Domestic Violence, Dating Violence, Sexual Assault & Stalking.

For many survivors of intimate partner violence and abuse, their privacy and confidentiality is paramount to their safety. Victim service agencies play a significant role in ensuring that confidentiality and safety. Revealing personally identifying information about survivors who seek services or the details of their abuse to anyone without the survivors' permission or knowledge can jeopardize their path to safety.

Frequently Asked Questions

Answers to common questions on releases and waivers, U.S. Federal laws on confidentiality, record retention and deletion, and more.

Templates

Sample template policies, including policy guidelines and sample MOUs for co-located programs and community collaborations, that victim service agencies can adapt and use.

Tipsheets & Charts

Handouts on technology, safety and confidentiality, including tip sheets on cell phones and location, online privacy tips, guidelines on selecting databases, and more.

Appendices

References to Federal laws, confidentiality information from U.S. government agencies, and other resources on confidentiality and privacy.

Technology & Confidentiality Toolkit

App Safety Center

Resources

- 10 Steps for Presenting Evidence in Court https://www.ncjfcj.org/10-Steps-Presenting-Evidence
- Judges' Awareness, Understanding, and Application of Digital Evidence http://www.garykessler.net/library/kessler_judges&de.pdf
- Mobile devices: New Challenges for Admissibility of Electronic Evidence https://www.americanbar.org/content/dam/aba/events/science_technology/mobiledevices_new_challenges_admissibility_of_electronic_device.authcheckdam.pdf
- "Connected" Discovery: What the Ubiquity of Digital Evidence Means for Lawyers and Litigation http://jolt.richmond.edu/2016/04/01/connected-discovery-what-the-ubiquity-of-digital-evidence-means-for-lawyers-and-litigation/

NNEDV
Tech Safety

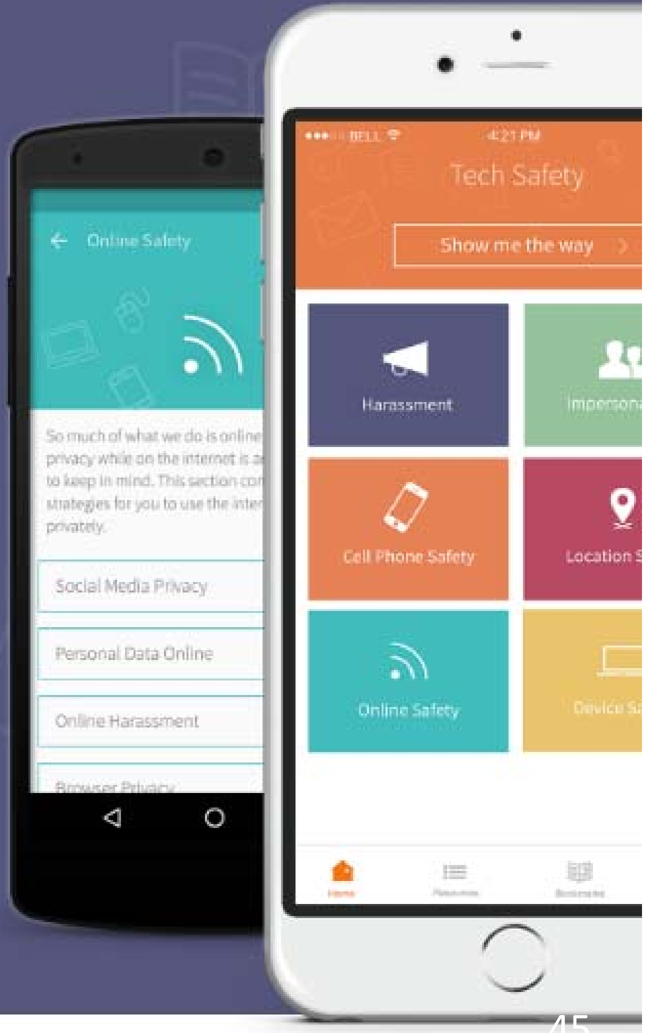
TechSafetyApp.org

Tech Safety

Welcome to the Tech Safety App. This app contains information that can help someone identify technology-facilitated harassment, stalking, or abuse and includes tips on what can be done.

Download on the App Store

Get it on Google play



Contact Information

The Safety Net Project at the National Network to End Domestic Violence:

- Safety Net Team email safetynet@nnedv.org
- Ian Harris iharris@nnedv.org

NNEDV online technology safety resources:

- Toolkits and Safety Net Blog: techsafety.org
- National Network to End Domestic Violence: nnedv.org
- Women's Law: WomensLaw.org