Technological Abuse: Practical Considerations and Evidentiary Issues

Presented by:
Ian Harris, JD, MA
How to use this technology

- Raise hand
- Text chat
- Feedback

Please send a private chat message to Alice Wolfkill for help.

Call iLinc Technical Support at 800.799.4510.
The mission of the Stalking Resource Center is to enhance the ability of professionals, organizations, and systems to effectively respond to stalking.

The Stalking Resource Center envisions a future in which the criminal justice system and its many allied community partners will effectively collaborate and respond to stalking, improve victim safety and well-being, and hold offenders accountable.

The Stalking Resource Center provides training, technical assistance, and resource materials for professionals working with and responding to stalking victims and offenders.
Stalking
resource center

www.victimsofcrime.org/src
202-467-8700
src@ncvc.org
Goals

This webinar will provide participants with an introduction to:

* Gathering Evidence of technological issues
* Admitting Evidence of technological abuse
* How State Civil & Criminal Courts have Dealt with the Admission of Technological Evidence
* Ethical Issues for Attorneys
* Federal and State Legislation Aimed to Protect Survivors of Stalking and Domestic Violence from Technological Abuse
*What Won’t Be Covered*

• How offenders stalk using technology
• For information on the use of technology to stalk:

www.victimsofcrime.org/src

**THE USE OF TECHNOLOGY TO STALK**

Cell phones. GPS. Computers. Did you know that these technologies can be dangerous weapons in a stalker’s arsenal? This self-paced, interactive course will give you a better understanding of how stalkers use these and other technologies to locate, harass, and surveil their victims. You will also identify steps to assist in investigating stalking crimes and supporting victims of stalking.

SIGN IN
Username: 
Password: 
Log In  Forgot your password?

REGISTER »

This online training was produced by the Stalking Resource Center of the National Center for Victims of Crime under 2009-S2-BF-K005, awarded by the Office for Victims of Crime, Office of Justice Programs, U.S. Department of Justice. The opinions, findings, and conclusions or recommendations expressed in this online training are those of the contributors and do not necessarily represent the official position or policies of the U.S. Department of Justice.

What is Technological Abuse?

Cyberstalking

vs.

Technological Abuse
“Technological developments which have facilitated ever faster communication...along with their many benefits, bring with them ever greater potential for abuse.”

Increased prevalence of technology

Importance of technology for the lives of survivors of intimate partner violence

Wealth of information available

This information is often deleted/erased

It can be difficult to admit this evidence

Effective dispositions frequently require technological safety provisions

Technological evidence can greatly decrease the number of cases that need to be litigated
Gathering Evidence
* Maintaining evidence is critical, especially if the survivor chooses to report to law enforcement
  * Counter-intuitive
    * If you get an upsetting email or text, what are you naturally inclined to do?
  * Provide victim/survivor early on with information on how to maintain evidence
Gathering Evidence

* Encourage survivors to keep a stalking log
  * Log each time a person knows too much
* Save messages (text and audio)
* Take pictures of text messages
* Make sure that Instant Messenger (IM) saves messages
* Take “Screen shots” or “screen captures” of information on a computer (also on some smart phones)
* Print IMs, Text messages, Email messages (with headers) and call logs
* Telephonic Technology

* Surveillance Technology

* Computer & Internet Technology
Gathering Tech Abuse Evidence

* Can it prove that the other person is wrong or that your client is right?
* What is the evidence?
* Where is it saved?
* Can client access it? (personally or through another person)
* Do you need it to be certified?
Telephonic Abuse

* Constant calls and hang ups or voicemails
* Constant Text messages (instant messages)
* Spyware
  * Mspy, Stealthgenie, Mobilespy, etc...
* Sexting
* Spoofing
  * Spoofcard.com, Telespoof.com, Itellas, VOIP etc.
* Surveillance

* **GPS** (Global Positioning System) - tracking via cell phones and other devices

* **Cameras** - Webcams, Nannycams, Spycams

* **Social Networking** sites that ask you to check-in (Google Latitude, Yelp, Grindr)
* Computers & Internet Abuse

* Changing passwords on computers and websites
* Gaining access to email accounts
  * Deleting emails; Sending fraudulent emails; Intercepting email
* Gaining access w/out consent to social networking sites
* Creating false virtual profiles on dating sites or pornographic sites
  * Posting sexual or pornographic images or text
* Geotagging
* Savevid Plugin
* Online Investigation
  * Intellius, IRB Search, Accurint, Merlin Information, Tracers Info, TLO, IQ Data, MasterFiles, PublicData

* Information Aggregation sites:
  * Spokeo
  * Others: friendfeed, MyLifeBrand, Fuser, hellotxt, MySocial24x7, AlertThingy, twirl, Flock, Profilactic, Xoopit, Socialthing, Iminta, Readr, Onaswarm, Whereisme, Oneswirl, Dipity, Zupme
Taking a Screen Shot

Print Screen Button
• Command-Shift-3: Take a screenshot of the screen, and save it as a file on the desktop
• Command-Shift-4, then select an area: Take a screenshot of an area and save it as a file on the desktop
• Command-Shift-4, then space, then click a window: Take a screenshot of a window and save it as a file on the desktop
• Command-Control-Shift-3: Take a screenshot of the screen, and save it to the clipboard
• Command-Control-Shift-4, then select an area: Take a screenshot of an area and save it to the clipboard
• Command-Control-Shift-4, then space, then click a window: Take a screenshot of a window and save it to the clipboard
Gathering Evidence

REMEMBER! Print out all of the information:

"From: First name, Last name
CB# xxx-xxx-xxxx
Received:
Feb 4, 09 10:02 am"
MAKE SURE TO PRINT EMAILS WITH THE MESSAGE HEADER!

A Message Header is a list of the servers and Internet Protocol (IP) addresses from which a message originated and through which it traveled to reach you.
This message contains confidential information and is intended only for the individual named. If you are not the named addressee you should not disseminate, distribute or copy this e-mail. Please notify the sender immediately by e-mail if you have received this e-mail by mistake and delete this e-mail from your system. E-mail transmission cannot be guaranteed to be secure or error-free as information could be intercepted, corrupted, lost, destroyed, arrive late or incomplete, or contain viruses. The sender therefore does not accept liability for any errors or omissions in the contents of this message which arise as a result of e-mail transmission. If verification is required please request a hard-copy version. This message is provided for informational purposes and should not be construed as legal advice or opinion.
Ian Harris
Staff Attorney
P 212.590.3906
E attorney@dayonenyc.org

Day One
P.O. Box 1507
Canal Street Station
New York, NY 10013
P 212.566.8120 / 800.214.4150
F 212.566.8121
W www.dayonenyc.org

This message contains confidential information and is intended only for the individual named. If you are not the named addressee you should not disseminate, distribute or copy this e-mail. Please notify the sender immediately by e-mail if you have received this e-mail by mistake and delete this e-mail from your system. E-mail transmission cannot be guaranteed to be secure or error-free as information could be intercepted, corrupted, lost, destroyed, arrive late or incomplete, or contain viruses. The sender therefore does not accept liability for any errors or omissions in the contents of this message which arise as a result of e-mail transmission. If verification is required please request a hard-copy version. This message is provided for informational purposes and should not be construed as legal advice or opinion.
Evidentiary Issues
Technology and Evidence: A Primer

Evidence and Case Law

- Telephonic Technology
- Surveillance Technology
- Computer & Internet Technology
- Subpoenas
- Dispositions
Technology may present complicated issues, but the rules are the same

* The Good News: Technology frequently provides evidence where none existed before
* The Bad News: Technology, while generally reliable, may allow for anonymous or fake evidence
* Nothing disappears online, but it may be difficult to locate
* Using technology to harass or abuse somebody can have major emotional and physical repercussions
1. Is evidence **relevant**? (Rule 401)
2. If relevant, is evidence **authentic**? (Rule 901)
3. If offered for substantive truth, is it **hearsay**? (if so, is there an exception?)
4. Is the evidence an **original or duplicate** under the original writing rule? (is there admissible secondary evidence to prove the content)
5. Does the **probative** value substantially outweigh the danger of unfair prejudice.
Why are the parties seeking to admit the evidence?

1. Admission by Party Opponent
2. Prior Inconsistent Statement
3. Present Sense Impression
4. Etc...
Most courts “require the production of an original writing where its contents are in dispute and sought to be proven.”

What if there is not an “original?”
"[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."
The owner or possessor of a telephone has the “right to be free of unwanted text messages. The brevity of a text message has no impact on the severity of its meaning. A short text message can be more vicious and threatening then a lengthy, convoluted e-mail or letter…”


* What is a Text message?
* Form of Text Message Evidence:
  * Screenshot or digital photo
  * Phone or Computer
  * Records from Phone or Messaging Company
  * Print out, cut-and-paste, or handwritten transcript
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)
Cases (Various Jurisdictions):

- “Authenticity can be shown through the testimony of a participant to the conversation that the document is a fair and accurate representation of the conversation” United States v. Gagliardi, 506 F.3d 140 [2d Cir.2007];

- A participant to the conversation testified that the print-out of the electronic communication was an accurate representation of the exchange and had not been altered in any significant manner]” United States v. Tank, 200 F.3d 627 [9th Cir.2000];

- A handwritten transcript of text messages was properly authenticated through testimony from the recipient of the messages, who was also the creator of the transcript. State v. Roseberry, 967 N.E.2d 233 [Ohio 2011];

- Testimony from a participant to the conversation was sufficient. Jackson v. State, 320 S.W.3d 13 [Arkansas 2009].
**Authenticity and Reliability**

- “Court erred in admitting text message from cellular telephone [without] establishing authenticity or reliability of text message [and] permitting jury to access entire contents of cellular telephone. People v. Givans, 45 A.D.3d 1460 (NY Sup Ct. 2007)

- Failure to authenticate 10 out of 12 text messages was error. Evidence is needed to show not simply that messages came from a particular phone, but that the alleged author of the messages was the one who actually sent them. People v. Rodriguez, 128 Nev. Adv.Op 14, 273 P.3d 845 (Sup.Ct., Nev., 2012)

- Detective’s transcriptions of text messages on defendant’s cell-phone were not properly authenticated... prosecution offered no direct proof [from]testimony of recipients or other possible authors of the messages and the message contents did not provide any circumstantial evidence as to authorship; while text messages are unique to the cell-phone from which they were sent, the owner of the cell-phone does not necessarily have exclusive access to it. Commonwealth v. Koch, 39 A.3d 996 (Pa.Super.Ct., 2011) [Appeal granted, 44 A.3d 1147 (May 2012)]

**Anonymous and Fraudulent Text Messages**
“An individual has a substantial privacy interest in his or her telephone...the device is easily conceptualized as the functional equivalent of the mailbox.” The owner or possessor of the telephone has the “right to be free of unwanted telephone calls...”

People v. Shack, 536, 634 N.Y.S.2d 660, 658 N.E.2d 706

* Form of Phone Call Evidence:
  - Screenshot or digital photo of call log
  - Phone (call logs)
  - Records from Phone Company
  - Print out, cut-and-paste, or handwritten transcript
  - Recordings of messages left on voicemail
Form of Phone Record Evidence?
- Business Record
- Print out from litigants

What do Phone Records Include?
- Caller/Texter # and time of call/text
- Some Companies may have text content

Authentication?
- Business Records
- Testimony from account owner
- Testimony from third party witness
- Consent of parties
**Telephonic Evidence: Phone Records**

Other Considerations: Subpoenas

* **Opposing Party**
  - The third department noted that a party in a matrimonial action could not subpoena telephone logs and AOL instant messages chat logs without a showing that they are necessary for custody determination. Bill S. v Marilyn S., 8 Misc.3d 1013(A) (2005).

* **Nonparty**
  - The third department declined to sign a subpoena for third party phone records, noting that parties in a matrimonial action are not entitled to “disclosure against non-parties without ‘showing special circumstances’, i.e., that the information sought to be discovered is material and necessary and cannot be discovered from other sources’” Bill S. v Marilyn S., 8 Misc.3d 1013(A) (2005).
What is Surveillance?

* Videos
* Audio recordings
* GPS and other tracking records

Form of Surveillance Evidence:

* Video and audio recordings (on phones, other devices, and other storage formats)
* Print out of GPS and tracking information
* Surveillance Evidence

Authenticating Videographic Evidence

* Who can Authenticate?
  • Testimony of any person present when the activity occurred
  • Even without the person testifying, the remaining foundational elements have sufficient probative value to verify the film
**Foundation** New York courts have applied the standard for determining admissibility of photographs to evaluate the admissibility of video evidence.

- Identity of subject matter;
- Qualifications of operator who filmed the video or one who was a participant in the recording;
- Authenticity and accuracy-portrayal of a true, fair and accurate representation of events, people and/or scene depicted;
- Type and quality of film and video equipment;
- Manner of developing;
- Continuity of possession;
- Explanation of distortions or changes or editing; and
- Technical imperfections.

**People v Higgins, 392 N.Y.S.2d 800 [N.Y. Sup.Ct.1977]**
Testimonial evidence must come from a “witness to the recorded events, or of an operator or installer or maintainer of the equipment” or “by the photographer, or technician or engineer, or by any one who observed the events depicted” who can testify that the videotape “accurately represents the subject matter depicted.” *People v. Patterson 93 N.Y.2d 80 [N.Y. 1999]*;

Videographic evidence is only admissible if it is a true, fair, and accurate portrayal of events, people, and the scene depicted. *City v. Prophete 544 N.Y.S.2d 411 [N.Y. Civ.Ct. 1989]*.
A videotape is true, authentic, and accurate evidence if, among other indicators, the tape is filmed with quality video equipment and it is without distortion or deletion. *People v. Curcio* 645 N.Y.S.2d 750 [N.Y. Sup.Ct. 1996].

Skips or deletions must not be so substantial as to render the whole video untrustworthy. *People v. Gucciardo* 355 N.Y.S.2d 300 [N.Y. Sup.Ct 1974].

Plaintiff’s wedding video was relevant to claims that she could no longer engage in activities such as running or horseback riding, due to permanent injuries. *Sgambelluri v. Recinos*, 192 Misc 2d 777 (S. Ct., Nass. Cty.)
Anatomy of an Email Message
  • Header (Sender, Recipient, IP Addresses)
  • Body
  • Signature

Forms of Email Message Evidence:
  • Screenshot or digital photo
  • Phone/Computer
  • Records from Email Company
  • Print out, cut-and-paste, or handwritten transcript
**Who can Authenticate?**
- Person who saw the message (recipient, sender, or third party)
  - Testify what the message said and where it came from (screenshot or the actual phone/computer)
  - Testimony of what a deleted message said
- Email records (Business Record)

**How to Authenticate:**
- Proof that the email came from the alleged sender
  - Derived from an account available to or connected to the alleged sender
  - Alleged sender is responsible for the email being sent (Intentionally sent the message to the recipient, intentionally used a third party, and/or failed to act)

**Issues with Authentication:**
- Emails can be sent anonymously
- Emails can be “spoofed”
Retrieval of email messages from a person’s email account that party had access to is not considered “eavesdropping evidence” and therefore not subject to exclusion under CPLR 4506(1). Gurevich v Gurevich, 24 Misc.3d 808 (2009)

Violation of no contact Order of Protection that Respondent knew or intended that, by sending the e-mail to the Petitioner’s family, it would reach the Petitioner. Matter of Jennifer G. v Benjamin H., 84 A.D.3d 1433 (2011); see also Matter of Duane H. v Tina J., 66 AD3d 1148, 1149 [2009].

Email messages sent by computers, cell phones and/or other devices items can constitute aggravated harassment in the second. Matter of Julie G. v Yu-Jen G., 81 A.D.3d 1079 (2011); M.G. v. C.G., 19 Misc.3d 1125(A) (2008).
* Respondent has a duty to ensure that he did not send Petitioner any e-mail messages, even through mass mailings. Odden v. Rath, 730 N.W.2d 590 (2007)

* Wife failed to demonstrate that husband was responsible for sending three threatening e-mail messages where the first message indicated that it came from wife's former (shared) account, the second originated from previously unidentified address, and the third was routed through wife's sister and only indicated that original message came from person by wife's name. Smith v. Smith, 24 A.D.3d 822 (2005).
Forms of Social Networking Evidence:

- Screenshot or digital photo
- Phone/Computer
- Records from Social Networking Company
- Print out, cut-and-paste, or handwritten transcript
Who can Authenticate?
- Person who saw the message (recipient, sender, or third party)
  - Testify what the message said and where it came from (screenshot or the actual phone/computer)
  - Testimony of what a deleted message said
- Records from Social Network Company (Business Record)

How to Authenticate:
- Proof that the posting/information came from the alleged sender
  - Derived from an account available to or connected to the alleged sender
  - Alleged sender is responsible for the information being sent (Intentionally sent the message to the recipient, intentionally used a third party, or failed to act)

Issues with Authentication:
- Posting can be sent anonymously
- Postings can be “spoofed”
- It is unclear who owns the information
Who Owns Social Networking Information?
Twitter had to disclose all non-content information and content information for Defendant. Defendant had no proprietary interest in the user information on his Twitter account and lacked standing to quash the subpoena. **People v. Harris 2012 N.Y. Slip Op. 22175.**

Discovery of Social Networking Accounts Permitted
Discovery of plaintiff's MySpace and Facebook accounts was material and relevant to plaintiff's claim that she could no longer participate in certain activities as a result of injuries. **Romano v. Steelcase Inc., 30 Misc 3d 426 (S. Ct. Suff. Cty.)**

Printout of Messages Admissible
Facebook message admitted into evidence showing that wife did not post pictures because they would hurt her legal claim. **B.M. v D.M., 31 Misc.3d 1211(A) (2011)**
* Libel and Defamation

Postings not libel where the postings were made on a “secret” Facebook group, which has no public content and does not appear on a Facebook member's profile. “Reasonable reader, given the overall context of the posts, simply would not believe that the posts are true.” **Finkel v Dauber, 29 Misc.3d 325 (Nassau Sup. Ct. 2010)**

* The Ability to Alter Photographs May Limit Admissibility

Defendant was not allowed to introduce pictures from MySpace in order to cross examine witnesses about their alleged gang membership “In light of the ability to “photoshop,” edit photographs on the computer, and defendant could not authenticate the photographs.” **People v Lenihan, 30 Misc.3d 289 (Queens Sup. Ct. 2010)**

* Proof of Intentional Harassment

18-year-old defendant could not be charged with aggravated harassment (Penal Law § 240.30 [1]) for having merely sent messages to the 14-year-old complainant through a social networking Web site expressing his unrequited love for her, in the absence of any allegation that the messages were intended to threaten, incite alarm or harass.” **People v Rodriguez, 19 Misc.3d 830, 860 N.Y.S.2d 859 (N.Y. City Crim. Ct. 2008)**
* Attorneys May advise Clients to Take Offensive Material off Social Networks; NY County Lawyers Assoc. Comm. On Professional Ethics Formal Opinion #745: (July 2, 2013)

* Obtaining Evidence From Social Networking Websites

A lawyer may not attempt to gain access to a social networking website under false pretenses, either directly or through an agent. The Assoc. of the Bar of the City of NY Committee on Professional and Judicial Ethics Formal Opinion 2010-2.
Lawyer’s Access to Public Pages of Another Party’s Social Networking Site for the Purpose of Gathering Information in Pending Litigation

A lawyer in pending litigation may access the public pages of another party's social networking website (such as Facebook) for the purpose of obtaining possible impeachment material for use in the litigation. *NYS Bar Association Comm. on Professional Ethics Opinion 843: (9/10/2010)*

*Jury Research and Social Media; Formal Opinion 2012-2*

*Lawyer Investigation of Juror Internet and Social Networking Postings During Conduct of Trial; NY County Lawyers Assoc. Comm. On Professional Ethics Formal Opinion #743: (May 11’)*
Using a Website to Communicate through 3rd Party

Defendant and a co-worker created a website containing suggestive photographs and words, and listing complainant’s address and telephone numbers with a request that people contact her. She was called twice at work. Defendant’s actions constituted criminal contempt and aggravated harassment in the second degree. A defendant is not exculpated because he, instead of placing the phone call to his victim himself, used others to do so. People v Kochanowski, 186 Misc.2d 441 (2000)

Threats on Public Website = Aggravated Harassment

Message on a computer Internet newsgroup which stated “Please kill Police Lt. Steven Biegel, all other NYPD cops, and all of their adult relatives and friends” was aggravated harassment where the officer felt scared. People v Munn, 179 Misc.2d 903 (1999)
**Computer Evidence: Orders of Protection**

* Friend Request Is a Violation

* Posting on Craigslist is a Violation
  Criminal contempt found where defendant, in addition to sending victim several violent emails, also posted on Craigslist the victim's name, address, license plate number, place of employment, make and model of her car and false allegations about her illegal immigrant status. People v. Phelan, 82 A.D.3d 1279, 918 N.Y.S.2d 608 (3d Dep't 2011), leave to appeal denied, 17 N.Y.3d 799, 929 N.Y.S.2d 107, 952 N.E.2d 1102 (2011)

* Contacting Facebook friends of Petitioner Not a Violation
  People v. Welte, 31 Misc. 3d 867, 920 N.Y.S.2d 627 (J. Ct. 2011)
Computer Memory is Akin to a File Cabinet

“Plaintiff did not act illegally by removing the ‘family’ computer from the marital residence. Plaintiff wife is entitled to access to information concerning defendant husband's finances and personal business records stored in a laptop computer owned by defendant's employer but kept by defendant in his home...Computer memory is akin to a file cabinet and plaintiff clearly could have access to the contents of a file cabinet left in the marital residence.” Byrne v Byrne, 168 Misc.2d 321 (1996)

May Have Access to Hard Drive of Family Computer

Wife's access to material downloaded and saved to the hard drive of the computer found by the wife in the trunk of her husband's car was not the result of an intercepted communication and does not constitute a violation of Penal Law § 250.05. Moore v Moore (NYLJ, Aug. 14, 2008, at 26, col 1 [Sup Ct, NY County]). See also Boudakian v Boudakian (NYLJ, Dec. 26, 2008, at 27, col 3 [Sup Ct, Queens County 2008]) and Gurevich v Gurevich, 24 Misc.3d 808 (2009).

Access Should Not be Unrestricted

Wife's allegations that defendant husband concealed and misrepresented his income and assets were insufficient to justify the unrestricted turnover of defendant's office computer hard disk drive. Schreiber v Schreiber, 29 Misc.3d 171 (2010)
Subpoenas Regularly Signed by Judges for Tech Evidence

- Identity of account holder and communications obtained by service of a subpoena on the Internet service provider.” People v Foley, 257 A.D.2d 243 (1999).
- Family offense proceeding alleging that father sent vulgar messages to mother, court approved subpoena directing Yahoo!, to disclose only information identifying father as holder of the e-mail account and the contents of e-mail messages sent from that account to the mother's e-mail account during a designated time-frame. Matter of D.M. v. J.E.M., 873 N.Y.S.2d 447 (Fam. Ct., Orange Co., 2009)
- Subpoena of e-mails, telephone logs and three years of AOL instant messages chat logs to establish divorce grounds rejected as overbroad; court noted that more latitude is afforded to discovery regarding financials, as compared to grounds) Matter of Bill S. v. Marilyn S., 8 Misc.3d 1013(A) (Sup.Ct., Nassau Co., 2005)

Subpoenas May be Expensive

- Facebook subpoenas cost $150 and there are no domestic violence exceptions.
- Many telephone companies are similarly expensive.
Sample Language

- Observe such other conditions as are necessary to further the purposes of protection: respondent not to post any references to the petitioner on any internet site.
- “Refrain from communication or any other contact by mail, telephone, e-mail, voice-mail, or other electronic or any other means with ______ or through social network whether directly or through third parties. Respondent must refrain from disseminating, posting or distributing any sexually explicit photos, tapes or online recordings involving the Petitioner.”
Sample Language

• “No contact with petitioner through any method of communication including but not limited to cell phone, text message, email, regular mail correspondence, any social networking site such as Facebook, AIM “chat,” etc. or third person contact;

• “Observe such other conditions as are necessary to further the purposes of protection: Neither party to contact each other on Facebook or any other internet based social network. Both parties are to remove each other as “contacts/friends” from any internet based social network forthwith.” No 3rd party contact.
Based on posting of a video of an assault on MySpace in violation of condition of interim release, the court included a prohibition on computer use other than educational purposes. Matter of Ashley D., 55 A.D.3d 605 (2008)
Phone Calls & Letters Enough to Establish Personal Jurisdiction

- While “random, fortuitous, or attenuate contacts are not sufficient” to establish ‘minimum contacts’ under a long-arm statute, courts must consider the “nature and quality of actions.” The abusive actions taken was not like circumstances surrounding business transactions by mail and/or phone and because the acts repeatedly had their effect in another state, that was sufficient to establish minimum contacts. Beckers v. Seck 14 S.W.3d 139 (2000)

Purposeful Injurious Actions Can Establish Personal Jurisdiction

- “A forum may assert specific jurisdiction over a non-resident defendant where an alleged injury arises out of or relates to actions by the defendant himself that are purposefully directed toward forum residents, and where jurisdiction would not otherwise offend ‘fair play and substantial justice.’” Burger King v. Rudezewicz 471 U.S. 462 (1985)
RESOURCES
Resources for Survivors

* Safe Shepherd - www.safeshepherd.com/advocates
  * Free premium service for stalking victims

* Reputation.com
  * Free service for domestic violence victims

* NNEDV - The SafetyNet Project - www.nnedv.org
  * Survivors & Technology: An Interactive Safety Planning Tool

* That’s Not Cool - www.Thatsnotcool.com

* A Thin Line - www.Athinline.org
Resources for Law Enforcement

* Regional Information Sharing Systems
  * www.riss.net

* Regional Computer Forensics Laboratory
  * www.rcfl.gov

* Justice Technology Information Network
  * www.justnet.org

* Electronic Crime Technology Center of Excellence
  * www.ectcoe.net

* Search.org
Resources for Law Enforcement

* Electronic Crime Scene Investigation: An On-the-Scene Reference for First Responders, November 2009
* Investigations Involving the Internet and Computer Networks, January 2007
* Forensic Examination of Digital Evidence: A Guide for Law Enforcement, April 2004

Available at http://victimsofcrime.org/src/resources/for-practitioners#cjs
Training

- In person training
- Webinars

Technical Assistance

- Individual & organizational assistance
- Fact sheets, brochures, manuals, guides
- Policy/protocol development & consultation
- Videos
- Online resources
- Stalking Awareness Month materials

Resources

www.victimsofcrime.org/src
Questions?
Legal Ecosystem
Legal Ecosystem

* Federal Law

- The Electronic Communications Privacy Act (ECPA) (18 U.S.C. § 2501)
- Federal Stalking Law (Interstate Communications) (18 USC § 875)
- Obscene or harassing telephone calls (47 USC § 223)
- Violence Against Women Act (VAWA)
  - Interstate domestic violence (18 USCS § 2261)
  - Stalking (18 USCS § 2261A)
Federal: Electronic Communications Privacy Act (ECPA)

* Purpose:
Makes it **unlawful** for a person to **intentionally intercept** any wire, oral, or electronic communication, or to **use** or **disclose** any wire, oral, or electronic communication that has been intentionally intercepted.

* Penalties:
Criminal Penalty: fine or imprisonment of not more than five years, or both. Civil actions are permitted

* **NOTE**: May be Permissible to intercept any wire, oral, or electronic communication if: 1) party to the communication or 2) one of the parties to the communication gives prior consent.

* **NEW LEGISLATION**: Online Communications and Geolocation Protection Act was recently introduced in Congress. (H.R. 983)
Federal: Stored Communications Act (SCA)

18 USC Chapter 121 §§ 2701–2712

* Purpose:
Makes it unlawful to intentionally access, without authorization, an electronic communication service or... intentionally exceed an authorization to access that facility. The Law also describes the conditions under which the government is able to compel disclosure of "customer or subscriber" content and non-content information for each of these types of service (§ 2703). Applies to:
- “Electronic communication services” (any service which provides to users the ability to send or receive wire or electronic communications) and
- “Remote computing services" (Any service that provides the public with computer storage or processing services by means of an electronic communications system).

* Penalties:
- Criminal Penalty: fine or imprisonment of not more than five years, or both. Civil actions are permitted
Purpose:
Prohibits the intentional interception, use, or disclosure of wire and electronic communications. Bars third parties (including the government) from wiretapping telephones and installing electronic "sniffers" that read Internet traffic.

Penalties:
Criminal Penalty: fine or imprisonment of not more than five years, or both. Civil actions are permitted

NOTE:
There are statutory exceptions, such as a properly secured warrant for a wiretap.
Purpose:

875(C) Prohibits transmitting in interstate or foreign commerce any communication containing any threat to kidnap any person or any threat to injure the person of another.

Penalties:

Criminal Penalty: fine or imprisonment of not more than five years, or both. Civil actions are permitted.
Federal: Obscene or Harassing Telephone Calls

47 U.S.C. § 223

* **Purpose:**
Makes it a crime to use a telephone or telecommunications device to annoy, abuse, harass, or threaten.

* **Penalties:**
Criminal Penalty: fine or imprisonment of not more than two years, or both. (Misdemeanor)

* **NOTE:**
Broader than federal stalking law, because it covers threats and harassment.
* **Purpose:**
  A. Prohibits travel with the intent to kill, injure, harass, or intimidate a spouse, intimate partner, or dating partner, where in the course of or as a result of such travel or presence, commits or attempts to commit a crime of violence against that spouse, intimate partner, or dating partner.

  B. Prohibits causing a spouse, intimate partner, or dating partner to travel by force, coercion, duress, or fraud, and who, in the course of, as a result of, or to facilitate such conduct or travel, commits or attempts to commit a crime of violence against that spouse, intimate partner, or dating partner

* **Penalties:**
  Criminal Penalty: fine or imprisonment of not more than five years, or both. Civil actions are permitted.
18 U.S.C. § 2261A and b

* Purpose: § 2261A (Stalking)
Prohibits the use of “mail, any interactive computer service, or any facility of interstate or foreign commerce to engage in a course of conduct that causes substantial emotional distress to that person or places that person in reasonable fear of the death of, or serious bodily injury.”

* Purpose: 18 USC § 2261(b)
Increased penalties for those who stalk while subject to a civil protection or restraining order.
* State Laws

* Penal Law
  * Will vary from state to state
    * All state stalking and related statutes available at www.victimsofcrime.org/src

* Evidence
- Eavesdropping (P.L. §250.05)
- Unauthorized Use of a Computer (P.L. §156.05)
- Computer Trespass (P.L. §156.10)
- Computer Tampering (4th – 1st degree) (P.L. §156.20 - §156.27)
- Stalking (P.L. §120.45)
- Unlawful Surveillance (P.L. §250.40)
- Tampering with private communications (P.L. § 250.25)
- Dissemination of an Unlawful Surveillance Image (P.L. §250.55)
- Disseminating Indecent Material to Minors in the first and second degree (P.L. §235.21 -§235.22)
- Criminal Mischief in the fourth degree (P.L. §145.00)
• **Aggravated Harassment in the Second Degree** (P.L. §240.30)
  • (a) communicates with a person, by mechanical or electronic means or otherwise, or causes a communication, anonymously or otherwise, by telephone, by telegraph, or by mail, or by transmitting or delivering any other form of written communication, in a manner likely to cause annoyance or alarm

• **Harassment** (P.L. §240.25)

• **Menacing** (P.L. §120.14)

• **Disorderly Conduct** (P.L. §240.20)
• Eavesdropping evidence (CPLR §4506 (1))
  • Eavesdropping evidence obtained in violation of Penal Law § 250.05 may not be received in evidence

• Privileged communications; electronic communication thereof (CPLR §4548)
  • No privileged communication shall lose its privileged character for the sole reason that it is communicated by electronic means

• Business records (CPLR §4518)
  • An electronic record shall be admissible in a tangible exhibit that is a true and accurate representation of such electronic record.

• Best Evidence Rule CPLR 4539(b):