

## USE OF SOCIAL MEDIA IN TEEN DATING VIOLENCE: TECHNOLOGY “HOW-TOS” FOR JUDGES

### *How to Stay Up-to-Date on TDV Issues*

Technology is constantly changing and new apps gain popularity rapidly. The platforms included in this fact sheet are the latest list, but are subject to change.

- **Break the Cycle** is updated regularly with current issues (<http://www.breakthecycle.org>).
- **Futures Without Violence** has a number of helpful Fact Sheets (<http://www.futureswithoutviolence.org/resources-events/get-the-facts>).
- The **National Network to End Domestic Violence** (NNEDV) has a thorough list of resources (<http://nnedv.org/resources.safetynetdocs.html>).

### *How to Retrieve Messages from Smartphones*

- Applications that victims or law enforcement officials can download to recover text messages that have been deleted from a smartphone:
  - Recover, Wondershare, Dr. Fone, TextRar
- Contact cell phone carriers (Verizon, Sprint, etc.) to access their databases of information from personal cell phones.
- Search other electronic devices, such as laptops or tablets
  - Apple has a "**cloud**" **server** where it automatically saves information from electronic devices.
  - Apple iPhones typically upload text message content to computers, laptops, and tablets when they are connected to one another (e.g. when a phone is synced with iTunes)
  - You do not have to manually save something to the cloud for it to save there - most companies make the save function automatic
- Search other individuals' electronic devices (including the victim's)
  - When a Google "Hangout" history (instant message conversation) is deleted from a computer, it will be deleted from the user's Gmail account and mobile devices, **but other people who participated in the Hangout can still view the history.**<sup>35</sup>
- How to collect cell phone evidence:
  1. Use time stamp features
  2. Request information from service providers
  3. Advise parties with Orders of Protection to use **screen shots** to capture text messages, emails, and photos ("snaps") that can expire
  4. Refer to telephone bills and bank statements to view costs and outgoing calls<sup>36</sup>
  5. In some cases, authorities have successfully obtained the records of notoriously hard-to-track prepaid cell phones<sup>37</sup>

\*This project was supported by Grant No. 2013-TA-AX-K043, awarded by the Office on Violence Against Women, U.S. Department of Justice. The opinions, findings, conclusions and recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the views of the Department of Justice, Office on Violence Against Women.

## ***How to Obtain Information That May Be Open to “E-discovery”***

- For many websites, law enforcement officials can subpoena Internet service providers and view Web site logs to obtain criminal evidence
  - [www.search.org](http://www.search.org) has contact information for many web site hosts and other technology service providers
- The federal Stored Communications Act (SCA)<sup>38</sup> allows social media providers to refrain from divulging private communications, even in response to civil subpoenas.
  - To access communications on Facebook, Twitter, and Google+, follow the request channels of those providers.<sup>39</sup>
    - **Facebook:** Users click the "Download a copy of your Facebook data" link, and the company will send the user his/her site history
    - **Twitter:** all "tweets" are publicly viewable and catalogued with date and time stamps
      - Public tweets can also be located on websites such as AllMyTweets.net
      - Direct messages to individuals are not available to the public.
      - To see direct messages, Twitter provides instructions at <http://support.twitter.com/articles/1406-posting-or-deleting-direct-messages>
    - **Google+:** obtain information through <https://support.google.com/takeout><sup>40</sup>
- Email information can be traced through **IP (Internet Protocol) addresses** located in the email header.
  - IP addresses trace what streams information travelled to and from where

## ***How to Ensure Teen Victims are Protected***

- Teen victims may fail to follow recommendations to refrain from using a form of technology to avoid the abuse or stalking.
  - Instructing a victim to shut down her Facebook account will not end the abusive behavior; the perpetrator will find another means of harassment and control.<sup>41</sup>
  - Cutting victims off from their online community removes their support network.<sup>42</sup>
  - Continued online presence can enable the victim to monitor continued abuse, which she can subsequently report.
- Victim-centered responses from legal professionals provide necessary assistance while facilitating continued involvement in academic and social activities necessary for growth and happiness.<sup>43</sup>
- List of possible communications to include in adolescents' orders of protection against abusive partners:
  - "No calling, no texting, no emailing any account belonging to the petitioner, no Facebook 'poking,' messaging or posting, on the petitioner's wall or about the petitioner on another individual's wall, no communication via Instagram, Snapchat, or any other social networking site or app."
  - Judges can order that perpetrators give them (or a probation officer) access to the perpetrators' electronic devices and social media passwords.<sup>44</sup>

- For teens in particular, it may be useful to quiz them so they understand that any electronic communication violates the OP
- e.g. "Would posting an old picture of you as a couple on Facebook violate the order?"
- Even when contact between parties is necessary or inevitable (e.g., attending school, sharing parental duties), limitations can be placed on communication or sharing personal information.
  - "For example, even if the order already prohibits electronic contact, the prohibition may also specify that the stalker not access computers or phones used by the victim or contact the victim through email or social networking services."<sup>45</sup>

### ***How to Evaluate ESI (Electronically Stored Evidence)***

- Federal Rule of Evidence 901(b) provides examples of how to determine whether evidence is authentic.
  - Example number (4) includes "appearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances."<sup>46</sup>
  - Be on the lookout for idiosyncratic abbreviations, **emojis** (picture symbols), nicknames or pet names, or inconsistent subject matter in determining whether the alleged author did, in fact, write the message in question.
- If there is even a chance that a cell phone contains electronic evidence, a judge can place a **litigation hold** on the cell phone.
  - Courts have increasingly turned to sanctions if litigation holds on electronic devices are violated.<sup>47</sup>

### ***Endnotes***

1. Google *Hangouts Help*, <https://support.google.com/hangouts/answer/3112001?hl=en>.
2. Cynthia Fraser, et al., *The New Age of Stalking: Technological Implications for Stalking*, JUV. & FAMILY CT. J. 61, no. 4 (Fall, 2010) at 43.
3. *Id.* at 42.
4. 18 USCS § 2701-12.
5. Hon. Matthew A. Sciarrino, Jr., *Social Media's Impact on Criminal Law*, § 2.1, KINGS CNTY CRIMINAL BAR ASSN., Oct. 17, 2013.
6. *Id.*
7. Fraser, et al., *supra* note 2 at 43.
8. Andrew Sta. Ana & Stephanie Nilva, *Teen Victims of Intimate Partner Violence*, 386, N.Y. LAWYERS MANUAL ON DOMESTIC VIOLENCE, (SIXTH) (forthcoming).
9. Eugene M. Hyman, et al., *In Love or In Trouble: Examining Ways Court Professionals Can Better Respond to Victims of Adolescent Partner Violence*, JUV. & FAMILY CT. J. 61, no. 4, 21-22 (Fall 2010) at 33.
10. See *People v. Ebertowski*, 228 Cal. App. 4th 1170, 11177 (2014) (holding that the probation conditions that defendant provide social media passwords and submit to searches of his electronic devices were reasonable).
11. Fraser, et al., *supra* note 2 at 49.

12. Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534 (D. Md. 2007) at 544.
13. Christou v Beatport, 849 F.Supp.2d 1055 (D. Colo., 2013) (imposing sanctions on defendant, who lost his iPhone after Plaintiff submitted a litigation hold letter, even though court found defendant's actions to be negligent and acknowledged the texts may not prove relevant); *see also* Gary M. Pappas, *Smartphones Can Be An E-Discovery Gold Mine or Sinkhole*, JDSupra Law News (2013); Zubulake v. UBS Warburg, LLC, 229 F.R.D. 422 (S.D.N.Y. 2004).